AIR FORCE, CYBERPOWER, TARGETING:
Airpower Lessons for an Air Force Cyberpower Targeting Theory

BY

STEVEN J. ANDERSON, LIEUTENANT COLONEL, USAF

A THESIS PRESENTED TO THE FACULTY OF
THE SCHOOL OF ADVANCED AIR AND SPACE STUDIES
FOR COMPLETION OF GRADUATION REQUIREMENTS

SCHOOL OF ADVANCED AIR AND SPACE STUDIES
AIR UNIVERSITY
MAXWELL AIR FORCE BASE, ALABAMA
JUNE 2013

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE
JUN 2013

2. REPORT TYPE

3. DATES COVERED
00-00-2013 to 00-00-2013

4. TITLE AND SUBTITLE
Air Force, Cyberpower, Targeting:Airpower Lessons for an Air Force Cyberpower Targeting Theory

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
School Of Advanced Air And Space Studies,,Air University,,Maxwell Air Force Base,,AL

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This thesis examines historical targeting theories for airpower and their effects on the Air Force organize, train, and equip functions. This analysis is intended to develop lessons learned in order to focus Air Force cyberpower organize, train, and equip functions. Just as early theorists conceptualized the use of airpower, so must the Air Force develop a cyberpower targeting theory to apply in future war.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a REPORT **unclassified**	b ABSTRACT **unclassified**	c THIS PAGE **unclassified**	**Same as Report (SAR)**	**163**	

APPROVAL

The undersigned certify that this thesis meets master’s-level standards of research, argumentation, and expression.

____

COLONEL M.V. SMITH

____

LIEUTENANT COLONEL RICHARD J. BAILY JR.

DISCLAIMER

The conclusions and opinions expressed in this document are those of the author. They do not reflect the official position of the US Government, Department of Defense, the United States Air Force, or Air University. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

ABOUT THE AUTHOR

Lieutenant Colonel Steven Anderson received his commission through the Officer Training School at Maxwell Air Force Base in April 1999. He is a cyberspace operator for the U.S. Air Force. His first commissioned assignment was at Robins AFB, Georgia where he performed combat airfield and combat support operations as a Maintenance Control Officer and Flight Commander. He then moved to Incirlik AB, Turkey where he was a Support Flight Commander, Group Executive Officer, and finally Wing Executive Officer. Next, Colonel Anderson attended the USMC Expeditionary Warfare School at Quantico MCB, Virginia, followed by a 2 year Pentagon tour as an Air Force Intern. Upon leaving D.C., he deployed for a year as the deputy commander, 380th Expeditionary Communications Squadron in the United Arab Emirates. Following this tour he performed officer assignment and force development duties related to cyber-operations at the Air Force Personnel Center, Randolph AFB, TX. In August 2009, Colonel Anderson assumed the duties as executive officer for the newly established Twenty-Fourth Air Force at Lackland AFB, TX. Next, he served as commander of the 3d Combat Communications Support Squadron at Tinker AFB, OK in June 2010 where he remained until his assignment to SAASS in June 2012.

Lieutenant Colonel Anderson has a B.A. in Management, Computer Information Systems from Parkville University, an M.B.A from Webster University of Missouri, and an M.A. in Organizational Leadership from The George Washington University in D.C. He is heading to the PACOM/J6 staff following graduation from the School of Advanced Air and Space Studies. He is blessed to be married to his wife and has three beautiful children.

ACKNOWLEDGMENTS

This thesis would not have been possible without the support of many truly remarkable people. I would like to offer my sincere appreciation to faculty and staff at the School of Advanced Air and Space Studies. This is an extraordinary academic institution and I am blessed to have been a part of it. In particular, I would like to thank my advisor, Colonel Michael 'Coyote' Smith. His guidance and insight helped shape the final product in many invaluable ways. I would also like to thank Lieutenant Colonel Richard Bailey for his perspective and critique of this work. Additional faculty at SAASS I would like to thank for supporting this thesis include Dr. Richard Muller, Dr. James Forsyth, Dr. Hal Winton, Dr. Stephen Wright, Col Suzanne Buono, and Lt Col David Woodworth. To my fellow classmates in Class XXII, thanks for making it a great year! I am humbled to have been included in such an outstanding group of leaders, officers, professionals, and strategists.

I would like to personally thank the many individuals who assisted in research or guidance toward subject material in support of this thesis. I apologize up front if I inadvertently left someone unrecognized, it was not intentional. In no particular order, I would like to thank: Major General Suzanne Vautrinot (24 AF/CC), Brigadier General Brad Shwedo (ACC/A2), Brigadier General (s) Robert Skinner (AFSPC/IG), Colonel Paul Welch (688 IOW/CC), Colonel Thomas McCarthy (Director, Center for Strategy and Technology), Dr. Kamal Jabbour (AFRL/RI), Dr. Richard Raines (AFIT/ENGE), Dr. Robert Mills (AFIT/ENG), Lt Col Aldwin Estrellado (AF/A3CF/A6CF), Lt Col Leonard Pilhofer (24 AF/A2X), Lt Col Michael Birdwell (91 NWS/CC), Lt Col Christian Basballe (USCYBERCOM), Lt Col Steven "Kuna" Lindquist (328 WPS/DO), Lt Col Scott Vickery (26 OSS/CC), Mr. Brian MacDougald (26 OSS/OSK), Maj Robert Biggers (Det 2, 318 IOG), Maj Jason Keen (AFJAGS), Maj Joel "Oz" Bieberlie (AFSPC/A3TW), and Mr. Steven Landes (NASIC).

I would like to give a special thanks to Colonel (retired) John Warden for taking time to meet and discuss his air campaign plan. His insight increased my understanding of the enemy as a system concept and directly contributed to this thesis.

I would like to thank my parents for instilling discipline, initiative, and a persistent drive throughout my early years; and the constant support to my family while serving the past 20 years in the Air Force. I also appreciate the many hours they spent reviewing SAASS papers throughout the school year, along with the countless iterations of this thesis.

To my wife, thank you for your constant support, understanding, patience, and love. When this adventure is done and we are on to the next, it is great to know we have shared every step of the way together.

Finally, I would like to thank my heavenly Father. I rely heavily on His word; specifically Philippians 4:13, "I can do all things through Him who gives me strength." I will continue to seek His counsel in all I do and pray I use the gifts He has given me according to His will.

ABSTRACT

This thesis examines historical targeting theories for airpower and their effects on the Air Force organize, train, and equip functions. This analysis is intended to develop lessons learned in order to focus Air Force cyberpower organize, train, and equip functions. Just as early theorists conceptualized the use of airpower, so must the Air Force develop a cyberpower targeting theory to apply in future war.

Following World War I, Airmen at the Air Corps Tactical School (ACTS) developed an "Industrial Web Theory" for targeting to achieve victory through airpower. This theory informed senior leadership decisions regarding organize, train, and equip functions for the Air Force throughout its use. The targeting theory was employed with mixed results from World War II through the Vietnam War. In the late 20th century, Colonel John Warden conceptualized and validated an airpower targeting theory based around a concept of the enemy as a system. This model earned its success in Operation DESERT STORM and is continually used in doctrine, education and training, and planning today. Although the Air Force went to war with the force it had in the early 1990's, Colonel Warden's theory informs organize, train, and equip decisions for senior leaders today.

An Air Force cyberpower targeting theory should consider lessons learned by early airpower theorists and practitioners. Just as Airmen attempted to influence the third warfighting domain during airpower's infancy and maturation, Airmen are attempting to influence the fifth warfighting domain of cyberspace today.

This thesis evaluates early airpower targeting principles and attempts to draw parallels in order to propose a cyberpower targeting theory. Next, the thesis draws upon limited artifacts inherent to wielding cyberpower—attribution, authorities, and centers of gravity—and acknowledges their impacts upon leaders and practitioners of cyberpower. Finally, the thesis proposes a cyberpower targeting theory based on offense, defense, and exploitation objectives. In addition to focusing on the adversary, the theory is intended to cause introspect in order to identify potential Air Force and national security vulnerabilities in, through, and from cyberspace.

CONTENTS

TABLE ILLUSTRATIONS

FIGURE ILLUSTRATIONS

Chapter 1

Introduction

Revolutionary change, fuelled by the information age, is occurring.

David Lonsdale

A major battle in a theater of operations is a collision between two centers of gravity; the more forces we can concentrate in our center of gravity, the more certain and massive the effect will be.

Carl von Clausewitz

On August 18, 2009 the United States Air Force activated Twenty-Fourth Air Force at Lackland Air Force Base, Texas. As General Kehler expressed, the focus of the service's newest numbered air force command was toward emerging requirements of cyberspace operations.[1] He went on to say that, "Through the Twenty-Fourth Air Force, our service will present a full spectrum of cyberspace capabilities vital to the joint warfighter."[2] Thus began the Air Force endeavor into what is called the "fifth operational domain" or "new frontier." [3]

Since the activation of Twenty-Fourth Air Force, there are many questions regarding Air Force cyber operations to ask. Is the Air Force any further along the path to providing the joint warfighter more operational capabilities within cyberspace than were available in 2009? Is the Air Force simply kicking the can down the road regarding operations and capabilities vice stopping to reflect and evaluate if we structured the force and defined objectives correctly and clearly from the beginning? Have the Department of Defense (DOD) objectives for cyberpower been clearly defined for the Air Force? Has the Air Force evaluated on-going cyber operations, and is Twenty-Fourth Air Force on the path the Air Force intended it to travel?

Comments by the Air Force's newest Chief of Staff, General Mark A. Welsh III, project a sense of caution as the Air Force moves forward in cyberspace. During the

[1] General Robert Kehler was the Air Force Space Command commander at the time Twenty-Forth Air Force was activated.

[2] See Carla Pampe, "Air Force activates cyber Numbered Air Force," Air Force Space Command, 18 August, 2009, http://www.afspc.af.mil/news/story.asp?id=123163863.

[3] See retired General Larry Welsh, *IDA Research Notes*, "Challenges in Cyberspace," Summer 2011, https://www.ida.org/upload/research%20notes/researchnotessummer2011.pdf. Also see Defense Secretary Leon Panetta speech to Business Executives for National Security aboard the Intrepid Sea, Air and Space Museum in New York. Zachary Fryer-Biggs, "Panetta Lays Out New Cyber Policy," *DefenseNews*, 12 October 2012, http://www.defensenews.com/article/20121012/DEFREG02/310120002/.

September 2012 Air Force Association Air and Space Conference and Technology Exposition, General Welsh said, “I still twitch when I say cyber. I’m a believer. I’m just not sure we know exactly what we’re doing in it yet and until we do, I’m concerned it’s a black hole.”[4] His brief comments capture succinctly not only what operators and leadership throughout the Air Force are thinking, but potentially what senior leadership throughout DOD and US civilian corporations ponder as well. These concerns are especially true during a period of fiscally constrained budgets, reduced government and corporate spending, unknown potential conflicts in the area of cyber, and its role in all warfighting domains.

The good news is, senior military leadership genuinely appears to care where cyber operations are going and are taking proactive measures to enable cyberpower efficacy. As recent as December, 2012, Lieutenant General Michael J. Basla, Air Force Chief Information Officer stated, “The Air Force needs to gain a better understanding of what the military as a whole will require in terms of cyber capabilities.”[5] He suggested this understanding would come from the Joint Chiefs of Staff and the Defense Secretary who plan to finalize US Cyber Command’s (USCYBERCOM) requirements in the coming weeks.[6] These comments and actions came within months of USCYBERCOM giving each armed service a list of cyber capabilities they were expected to execute in support of worldwide operations.[7] Now these tasks appear to be under review to ensure known and potential threats within the next decade are being addressed by each service’s required capabilities. The preceding statements signify a general acknowledgement of the extremely dynamic and evolving nature of the cyber domain; far outpacing the rate of change in the other warfighting domains. This is supported by a constant reminder that

[4] See General Mark A. Welsh III., speech to the Air Force Association Air & Space Conference and Technology Exposition on 18 September 2012, http://www.af.mil/shared/media/document/AFD-120928-037.pdf.

[5] See article by Jared Serbu, “Air Force role just 1 piece of DOD’s cyber puzzle,” *Federal News Radio,* 3 Dec 12, http://www.federalnewsradio.com/398/3140801/Air-Force-gels-around-its-cyber-future.

[6] See article by Jared Serbu, “Air Force role just 1 piece of DOD’s cyber puzzle,” *Federal News Radio,* 3 Dec 12, http://www.federalnewsradio.com/398/3140801/Air-Force-gels-around-its-cyber-future**.**

[7] John Reed, “The Pentagon is tweaking the cyber capabilities it wants from the services,” *Foreign Policy, 30 Nov 12,* http://killerapps.foreignpolicy.com/posts/2012/11/30/the_pentagon_is_tweaking_the_cyber_capabilites_it_wants_from_the_services.

cyber is the only man-made domain; the land, sea, air, and space domains are physical and, unlike cyberspace, rather unchangeable.

The questions posed above do not have simple answers and this treatise does not intend to propose their solutions. This thesis does however intend to focus on what the author calls a center of gravity for Air Force cyber operations—the *theory of Air Force cyberpower targeting*. The intent of this theory is to address the question: W*hat is the target of USAF cyberpower?* More specifically, *does the airpower targeting strategy employed by the Air Force apply to the use of cyberpower?* The theory proposed could go beyond Air Force thinking to the other service components, the DOD, and all national cyberspace functions critical to United States National Security. It also may aid military leadership in their current thinking about what capabilities military services need to wield cyberpower in order to support political objectives of the future. These needs, once determined, should shape the on-going organize, train, and equip cyber force discussions.

Cyber-targeting and associated doctrine should be the center of Air Force cyber strategy and its plans to organize, train, and equip a force for full spectrum cyberspace operations. Without a clear objective of what the Air Force intends to target within cyberspace, whether the focus is defense, offense, or exploitation, it is difficult to understand how an organization can execute operations, how education and training is focused, and how equipment can be procured toward intended objectives. Without a strategic focus regarding what the Air Force intends to target with cyberpower, one may draw parallels to the famous passage in Lewis Carroll’s *Alice in Wonderland*.

> Alice came to a fork in the road. ‘Would you tell me please which way I should walk from here?’ she asked.
> 'That depends a good deal on where you want to get to,’ responded the Cheshire Cat.
> 'I don't much care where,' said Alice.
> 'Then it doesn’t matter which way you walk,' said the Cat.[8]

Understanding what targets cyber operations can affect is critical to deliberate planning or crisis planning. Without understanding the target, it is difficult to understand

[8] L. Carroll, *Alice's Adventures in Wonderland* (Mac Millan, 1869), 89.

how operations are expected to achieve their objective. In order to understand targeting objectives, we must first understand the parameters for conducting cyber operations, as currently defined, and then current targeting doctrine regarding DOD operations.

Policy & Doctrine Review

Title 10 is the United States Code (USC) which governs operations by the Armed Forces. Military activities in cyberspace are defined within Title 10 in that "Congress affirms that the Department of Defense has the capability, and upon direction by the President, may conduct offensive operations in cyberspace to defend our Nation, Allies, and interests."[9] Of course the above actions are subject to policy and legal constraints which govern the DOD, too include the Law of Armed Conflict, and the Title 50—War and National Defense.[10] A review of both Title 10 and Title 50 authorities reveals absolutely nothing regarding cyber targeting as it relates to what the DOD efforts are to focus on. In fact, the word "cyber" is mentioned only four times on two pages in Title 50 in which the Chief of Defense Nuclear Security is directed to provide for the Administrations cyber security.[11] Given the activation of USCYBERCOM in 2009, one might question whether this Title 50 task still belongs to the Chief of Defense Nuclear Security or to the commander, USCYBERCOM. The lesson drawn from this is simply that the political objective for military cyberpower endeavors is not clearly found in United States Code Title responsibilities at this time.

Delving down closer to military operations relative to targeting, a review of Joint Publication 3-60, *Joint Targeting*, defines a target as, "an entity or object considered for possible engagement or action."[12] This definition of a target provides focus to a cyber-operator who is tasked to organize, equip, and train a force required to meet the Title 10 objectives defined above—when focused solely on offensive operations. However, the

[9] See Federation of American Scientists, Intelligence Resource Program, "Congress Authorizes Offensive Military Action in Cyberspace in FY2012 Defense Authorization Act," [Sec. 954, Military Activities in Cyberspace], 12 December 2011, https://www.fas.org/irp/congress/2011_cr/cyberwar.html.

[10] See Federation of American Scientists, Intelligence Resource Program, "Congress Authorizes Offensive Military Action in Cyberspace in FY2012 Defense Authorization Act," [Sec. 954, Military Activities in Cyberspace], 12 December 2011, https://www.fas.org/irp/congress/2011_cr/cyberwar.html.

[11] Title 50 United States Code § 932, *War and National Defense*, 4 January 2012, http://www.law.cornell.edu/uscode/pdf/lii_usc_TI_50.pdf.

[12] Joint Publication 3-60, *Joint Targeting*, 13 April 2007, vii, http://www.aclu.org/files/dronefoia/dod/drone_dod_jp3_60.pdf.

clarity of what to target still appears vague. An analysis of Air Force Doctrine Document (AFDD) 3-60, *Targeting*, yields no further explanation. In fact, the last publication of this document from June 2006, which incorporated changes as of May 2011, does not contain the word "cyber."[13] Somehow the Air Force missed including the updated mission of air, space, and cyber as part of this doctrine's update.

A continued deep-dive into currently published doctrine on targeting, and one closer to Air Force operations, we look at Air Force Instruction 14-117, *Air Force Targeting*. Although this document was last published in May 2009, three months before the activation of Twenty-Fourth Air Force, the word "cyber" only appears once in the document main body. This document delegates responsibility for cyber targeting to Air Force Space Command (AFSPC) when it says, "AFSPC will act as the lead MAJCOM for space-related and cyber targeting issues."[14] Given the focus of this Air Force Instruction on Intelligence operations within the Air Force, its assignment of responsibility is not faulty. It is however irrelevant when guiding Air Force commanders toward building effective cyberpower strategies and capabilities.

Finally, a review of Air Force Doctrine Document 3-12, *Cyberspace Operations*, provides the most direct discussion regarding AF cyber operations and targeting with cyberpower.[15] Initial document discussions focus on the adversary's intentions regarding DOD targets before turning to theater operations. The closest advocacy we find in current Air Force doctrine states that during planning, Twenty-Fourth Air Force organizations will use the Commander Air Force Forces Forward (COMAFFOR) or Joint Forces Air Component Commander (JFACC) joint integrated prioritized target list and target nomination list for operations. In other words, determining Air Force cyber targeting objectives is not determined by the unit tasked with conducting Air Force cyber operations, but rather by on-going theater level operations. A level of deductive reasoning leads one to conclude that cyber targeting is derived from pre-existing targeting doctrine for air and space operations that existed before the activation of Twenty-Fourth Air Force or US Cyber Command. Given new capabilities in warfare in, through, and

[13] Air Force Doctrine Document (AFDD) 3-60, *Targeting*, Change 1, 28 July 2011.
[14] Air Force Instruction (AFI), 14-117, *Intelligence: Air Force Targeting*, 13 May 2009, 6.
[15] Air Force Doctrine Document (AFDD) 3-12, *Cyberspace Operations*, Change 1, 30 November 2011.

from cyberspace operations, it is valid to evaluate a cyber-targeting theory that examines offensive, defensive, and exploitation possibilities beyond existing doctrine.

Literature Review

Academic research used to support positions within this thesis is focused primarily from the birth of airpower through today. A review of the Inter-War period, World War II, Korean War, and Desert Storm intends to evaluate airpower targeting theories in order to develop a cyberpower targeting theory for today. Although many books, periodicals, on-line articles, interviews, and historical research is used, the three principal books used for the three time periods discussed are; *History of the Air Corps Tactical School 1920-1940*, *The Air Campaign*, and *Cyberpower and National Security*.[16]

Robert Finney's, *History of the Air Corps Tactical School 1920-1940*, captures the first efforts by Airmen to think, develop, and document airpower targeting strategies. Beginning with the Air Corps Tactical School (ACTS), senior leaders would organize, train, and equip the Army Air Corps for airpower operations in World War II and beyond. From the early airpower theorist Billy Mitchell, through the men who served at ACTS, the strategic bombing mantra enveloped the service's culture before and after it became a separate service in 1947. This airpower tautology remained throughout the Cold War era until a new airpower strategist emerged.

John Warden, a Vietnam combat veteran, learned early in his career the implications of fighting a war with unclear objectives and equipment necessary to achieve them. In *The Air Campaign*, Warden defines a targeting theory that transcends the works of ACTS, while employing early principles of the industrial web theory. Although not a predetermined intention, Warden developed a 5-ring model for an air campaign plan that served the 1991 DESERT STORM Operation. The model receives an update throughout this thesis thanks to a personal interview with Colonel Warden. Since DESERT STORM, airpower strategists continue to use the works of Mitchell, ACTS, and

[16] R.T. Finney and Center for Air Force History, *History of the Air Corps Tactical School, 1920-1940* (Center for Air Force History, 1955); John A. Warden III, *The Air Campaign: Planning for Combat* (iUniverse, 2000); F.D. Kramer, S.H. Starr, and L. Wentz, *Cyberpower and National Security* (Potomac Books Incorporated, 2009).

Warden for all levels of war planning and operations. However, tomorrow's airpower strategists must focus on more than airpower; a focus on cyberspace is required.

Cyberpower and National Security is a litany of illustrations regarding cyberpower challenges facing the US. More than twenty authors with varying backgrounds and experience offer relevant cyberpower perspectives. From policy recommendations, problem definitions, and preliminary cyberpower theories, to infrastructure, technology, security, and law enforcement issues, this book synthesis major challenges facing the US as it attempts to wield cyberpower in order to influence national security objectives.

Warfare

The character of war will change, but the nature of war does not.[17] War in its simplest form is succinctly stated by Carl von Clausewitz; "war is fighting."[18] Fighting, in turn, is a trial of moral and physical forces through the medium of the latter [in which] psychological forces exert a decisive influence on the elements involved in war.[19] This point is especially relevant today as some theorists, academics, military, and civilian leaders argue cyber war is going on today. This statement is controversial on the basis that a declaration of cyber war does not exist, whereas official protocol for declaring war was established after the Hague Convention of 1907.[20] This perceived requirement for war has become somewhat convoluted with the rise of non-state and terrorist actors, in concert with reduced barriers of entry into warlike acts such as flying aircraft into buildings with innocent civilians. Either way, nations are struggling for dominance in cyberspace—the newest warfighting domain.

[17] The art of war is the art of using the given means in combat; there is no better term for it than the conduct of war. The art of war includes all activities such as the creation of the fighting forces, their raising, armament, equipment, and training. Clausewitz, Howard, and Paret, *On War*: 127. A more contemporary summation of war is offered by David Lonsdale in The Nature of War in the Information Age, "War is a purposeful act of actual or threatened physical violence which takes place within a dialectic relationship." Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future*: 2.

[18] Clausewitz, Howard, and Paret, *On War*: 127.

[19] Clausewitz, Howard, and Paret, *On War*: 127.

[20] See the Hague Convention of 1907 on the Opening of Hostilities, "Declaration of War," found at http://en.wikipedia.org/wiki/Declaration_of_war. Additional info is found at http://www.icrc.org/ihl.nsf/FULL/185?OpenDocument.

Perhaps a pursuit for cyber dominance today is comparable to the Cold War when after World War II two super powers struggled for military dominance. Both the United States and Soviets competed for dominance in the atomic and then thermonuclear power arena, just as nations like the US, China, Russia, France, and others struggle over cyberpower today. The difference is that many people today do not believe the struggle for cyberpower portrays the same potential for catastrophe as a nuclear holocaust, nor have the urgency to resolve known cyberspace vulnerabilities. But a look at history will show that US citizens were not overly concerned about atomic weapons or their threats until government educated the mass populace and instituted protective measures like bunker-run drills and air raid sirens to initiate action.[21]

Arguments can be made that cyberspace vulnerabilities have the potential to cause catastrophic or accidental events if left unprotected, or when specifically targeted. For this reason, it is practical to educate society on vulnerabilities created in, through, and from cyberspace, while focusing military operations on specific targets for cyberpower use. Until vulnerabilities of targets are exposed, along with their propensity for destruction, the possibilities of a "cyber-Pearl-Harbor" or "cyber-9/11" exist.[22] This argument does not suggest this level of potential catastrophe will not exist in the future, but at least societies will not be surprised if and when they do occur.

As the United States prepares for cyberspace warfare, whether catastrophic or benign, the military will be expected by the public to protect citizens from adversaries' intent on doing harm, at least from non-domestic threats given today's legal constraints. The question for those charged with this protection and who have the ability to wield cyberpower is not simply whether or not the United States can win a war by attacking the National Information Infrastructure (NII) of an enemy, but what is the political objective levied upon the military to perform?[23] Does the military exist simply to protect the

[21] P.C. Craig, *Destroying the Village: The Prospect of Thermonuclear War in American Security Policy* (Columbia University Press, 1998).

[22] Defense Secretary Leon Panetta speech to Business Executives for National Security aboard the Intrepid Sea, Air and Space Museum in New York. See Zachary Fryer-Biggs, "Panetta Lays Out New Cyber Policy," 12 October 2012, http://www.defensenews.com/article/20121012/DEFREG02/310120002/. Information was also provided by General Shwedo, Director of Intelligence, Air Combat Command. Brigadier General Brad "BJ" Shwedo, interview by author, Maxwell AFB, AL., 2 November 2012.

[23] David Lonsdale's reference to NII focuses on warfare that is kinetic destruction compared to disruption of capabilities which lead to a desired strategic effect. Both are capable products of cyber warfare given

sovereignty of the nation and its capabilities? Does cyberpower exist for limited war in support of other warfighting domains? Or should cyberpower be a full-spectrum capability for use throughout all phases of military operations and across all warfare domains? Answering these questions will aid in determining what centers of gravity to attack with cyberpower in order to meet political objectives.

Foundational Definitions

For the purpose of this study, war is an act of opposing wills pressing upon one another by force, or the threat of force, in order to influence ones political objective upon another. This definition is not new, but rather derived from varying interpretations of war from well-known theorists such as Carl von Clausewitz, Sun Tzu, and Karl von Moltke.[24] It is critical to start with understanding war before developing a theory for cyberpower targeting, if the objectives of targeting are to have a focus. At the same time, a common understanding of war helps readers delineate what is warfare and what is preparation of the battlefield before objectives of war are pursued.

Cyber war can have as many interpretations as those who consider the terminology. Some of the disparity comes from the fact that cyber war in the new domain is less understood than all of the other warfare domains combined.[25] Other disparity is derived from various threats within which cyber war exists. Threats vary from the national level (nation-states) to the individual level (hacktivists). Dr. Sheldon in his "State of the Art: Attackers and Targets in Cyberspace" article did a phenomenal job

the authorities, intelligence, and tools. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future*: 135-36.

[24] Clausewitz defines war as a trinity (primordial violence—people, chance and probability—commander, and element of subordination—instrument of policy). Clausewitz, Howard, and Paret, *On War*: 89.; Sun Tzu states "war is a matter of vital importance to the state" and must be appraised in terms of five factors (moral influence, weather, terrain, command, and doctrine), S.T.S.B.G. Sunzi, *The Illustrated Art of War: The Definitive English Translation by Samuel B. Griffith* (Oxford University Press, 2005), 91. Karl von Moltke defines war as rough and violent but went on to say that a rapid conclusion of war undoubtedly constitutes the greatest kindness, D. Hughes, *Moltke on the Art of War: Selected Writings* (Random House Publishing Group, 1995), 22-24.

[25] To read a paper on understanding "key features of cyber operations and types of cyber battles/conflicts that are possible to include broadening beyond traditional military operations in cyber wars that are fought between state actors with traditional forces," see Office of the Director of National Intelligence, *The IC and Cybersecurity, Traditions, Boundaries, and Governance,* (Washington: August 2010), 193.

by describing briefly major groups of potential threats.[26] Although the threat may vary, the understanding of what constitutes cyber warfare should not. The term cyber war as it relates to this thesis is mostly captured by Richard Clarke in Cyber War. Clarke states cyber war is "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption."[27] While agreeing with this definition, for our definition we have expanded Clarke's definition to include penetration into any portion of the cyberspace domain, or other warfighting domains supported by cyberpower, with the intent to cause damage or disruption to objects or loss of life. This association to a loss of life is highlighted in the Tallinn Manual in regards to its definition of a cyber-attack. The Tallinn Manual describes a cyber-attack as, "a cyber-operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects."[28]

The narrowing of cyber warfare specifically to a nation's computers or networks is too constrained given the reliance and inter-connectedness of DOD operations within cyberspace. Nuclear command and control, military command and control, logistics, transportation, security forces alert and response, Federal Aviation, financial, medical, and the list goes on, are all inter-connected through cyberspace and relied upon by DOD, commercial industry, and society alike. An attack on the New York stock exchange that cripples the nation's financial network might not be considered an act of war. However, an attack by one nation against another nation's major oil company which destroys 30,000 computers might be.[29] As a nation, the US should define what constitutes an act of war in, through, or from cyberspace and remove the ambiguity. This point is countered by those who argue that if cyber-laws are made unambiguous then nations are required to act against an adversary when a law is violated.[30]

[26] John B. Sheldon, "State of the Art: Attackers and Targets in Cyberspace," *Journal of Military and Strategic Studies*, 14, no. 2 (2012): 6-11.

[27] R.A. Clarke and R. Knake, *Cyber War: The Next Threat to National Security and What to Do About It* (HarperCollins, 2010), 6.

[28] M.N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, 2013), 106.

[29] See article, "Israel builds up its cyberwar corps," UPI.com, November 2012, http://www.upi.com/Business_News/Security-Industry/2012/11/02/Israel-builds-up-its-cyberwar-corps/UPI-52421351881449.

[30] See article by retired Major General Charles Dunlap where he argues cyber laws should be left somewhat ambiguous so that it is a political decision to react and not one you are forced into. This author argues that

Ultimately, to put cyber war in context, it is the decision of those governing each nation, in concert with their stated policy, while considering international law and precedence at the time, whether a specific cyber-attack is defined as warfare. This porous definition is attributed to the newness of the domain and does not account for the concerns today of attribution—being able to identify with certainty who actually conducted the attack.[31] The start of cyber war is not as clear cut as attacking a row of battleships as at Pearl Harbor on December 7, 1941, or marching an entire division of troops across the Kuwaiti border as Saddam Hussein did on August 2, 1991.

A final definition addressed up front is center of gravity; although it will be expanded upon in chapter 4. According to Clausewitz, identifying the centers of gravity is the first task in planning for war.[32] Applicable both to war and targeting, identifying centers of gravity enables efficacy in operations. This is applicable to cyber operations just as it applies to land, sea, air, and space operations. If organizations pursue capabilities (i.e. weapons or weapon systems in the case of a military), or conduct education and training, or exercises without identifying objectives, why should they expect to achieve desired results?

Since the focus is on military objectives, and accepting that in a democratic society like the US military objectives are always politically oriented, the targets of any military objectives should be focused on centers of gravity. As Joint Publication 5-0, *Joint Operations Planning* suggest, for a decisive response the priority of effort should be focused on the enemy center of gravity.[33] It goes on to say a center of gravity is the source of power that provides moral or physical strength, freedom of action, or will to act.[34] Clausewitz would say that “it is against these [objectives] that our energies should

whether laws are ambiguous or unambiguous, war is always left to a political decision. Militaries do not react when a law is violated without approval from civilian leadership. The reality is, unambiguous laws afford adversaries room to maneuver they might not otherwise have with defined laws. Charles Dunlap, “Perspectives for Cyber Strategists on Law for Cyberwar,” *Strategic Studies Quarterly* (Spring 2011): 81.

[31] For concerns about attribution and recommendations for addressing these on-going concerns see Patrick Lin, Fritz Allhoff, and Neil Rowe, “Is It Possible to Wage a Just Cyberwar?,” *The Atlantic*, 5 June 2012, http://www.theatlantic.com/technology/archive/2012/06/is-it-possible-to-wage-a-just-cyberwar/258106/#.UKJ8Z_mRMQ0.email. Some pundits suggest mandating that all cyberattacks should carry a digital signature of the attacking organizations. Although a utopic idea, the ability to enforce the idea borders impossible without international standards and a policing force to ensure compliance.

[32] Clausewitz, Howard, and Paret, *On War*: 619.

[33] Joint Publication 5-0, *Joint Operation Planning*, 222.

[34] Joint Publication 5-0, *Joint Operation Planning*, 250.

be directed"[35] since the "center of gravity is always found where the mass in concentrated most densely."[36]

As theories of warfare mature and interpretations vary, our definition of center of gravity takes into account the works of Dr Joe Strange, Professor of Strategic Studies at the USMC War College, as well as references provided above. Dr Strange's work toward bridging the gap between analyzing centers of gravity and their associated critical vulnerabilities by introducing critical capabilities and critical requirements is instrumental.[37] This is especially evident in the age of cyber-warfare where centers of gravity are not necessarily determined by concentrated mass as suggested by Clausewitz, but rather the interdependence of mass and operations supported in, through, or from cyberspace operations. Therefore, the working definition of center of gravity for this thesis is the source of power that inter-connects and enables psychological, moral, capabilities/physical strength, freedom of action, or an adversary's will to act. Although this definition is only a minor change from the JP 5-0 definition above, it draws upon the recognition that there is potentially more than one center of gravity, that their connectedness may be a center of gravity. It therefore opens the door for potentially greater psychological impact on the will of an adversary and possible exploitation to potentially prevent, or rapidly conclude an on-going war. This will become more relevant throughout the treatise in that the author believes cyberpower is an effective psychological warfare tool, in addition to being a supported, supporting, and decisive capability depending on the objective.

Thesis Intent

With the nature of war, cyber warfare, and center of gravity defined, and a known objective of this paper to develop a cyberpower targeting theory that helps shape Air Force objectives to organize, train, and equip its cyber forces, a historical review is in order to determine lessons learned from the latest domain used for warfare. Note that space is often referred to as the most recent domain for use by military; however, space is

[35] Clausewitz, Howard, and Paret, *On War*: 596.
[36] Clausewitz, Howard, and Paret, *On War*: 485.
[37] Jan Rueschhoff and Jonathan Dunne, "Centers of Gravity from the Inside Out," *Joint Forces Quarterly*, 60 (1Q, 2011): 120, http://ndupress.ndu.edu.

acknowledged as not being weaponized for warfare so comparisons to the air domain are appropriate here.[38]

Chapter 2 evaluates the ACTS studies on the industrial web theory to gain an understanding of airpower and its intended targeting effects during war. There are well documented studies on how early airpower strategists, and senior military leadership around the world, focused solely on strategic bombing as the dominant use for airpower. After World War II it became apparent to some, although not all, that changes were needed in aircraft, technology, training, and bombing tactics, techniques, and procedures if airpower was going to be the dominant form of warfare for which it was advocated. In reviewing the early history of airpower, questions surrounding cyberpower arise. Are cyber strategists faced with constrained advocacy for cyberpower capabilities? Or is the aperture opened fully to exploit all possibilities within cyberspace?

Chapter 3 continues a historical examination of airpower through a modern lens. An analysis of Colonel John Warden's look at airpower in the Twenty-First century provides an understanding of his five rings with the intention of gaining an in-depth understanding of its use in the theory of military strategic attack. As cyber strategists apply Warden's theories to the cyberspace domain, it is anticipated that commonalities exist in some areas, yet not in all. The expectation is that military strategists will avoid repeating mistakes learned through trial-and-error and avoid the cookie-cutter approach of applying theories of other domains collectively to the military's newest warfighting domain. As with any new warfare capability, on-going challenges in organization structure, manning, technology, domestic and international legal realms, as well as, education and training, and inter-service collaboration will persist for some time.

Chapter 4 highlights artifacts relevant to cyber operations. Specifically, it discusses the challenges of attribution and authorities, while acknowledging the required understanding of centers of gravity in cyber operations. Just as challenges existed when the effects of airpower were unknown, constraints exert themselves on the potential impacts of operations within cyberspace. Understanding these challenges may help

[38] For details regarding when an international agreement was established for banning the placement of all weapons of mass destruction in orbit around the earth, see information on the 1963 United Nations General assembly Resolution 1884. F.E. Morgan and Project Air Force, *Deterrence and First-Strike Stability in Space: A Preliminary Assessment* (RAND Corporation, 2010), 9.

answer similar questions developed in early days of airpower, while pressing cyberspace warriors to consider new ones not yet discussed. If addressing questions that inhibit operations today or potentially constrain future operations from achieving desired effects, then efforts to continually enhance cyber domain capabilities will be achieved. If cyberspace operators and strategists can discuss and debate serious questions such as, "What will cyber domain operations look like when the challenge of attribution is resolved?" or, "Can the barriers to entry into cyber operations be elevated to reduce potential threats?" then defenders of this nation's freedoms will be doing their job.

Chapter 5 leads us to a proposed cyberpower targeting theory that incorporates applicable lessons learned from other warfare domains while adding applicable thoughts specific to cyberspace operations. Unlike some early airpower advocates, the author's position is not one that states cyberpower is the dominant form of warfare. Nor is there extreme advocacy or debate over which form of cyber warfare, offense or defense, is the more capable position in cyber operations; although the author suggests more focus be placed on attributed offensive operations. The result is acknowledgement that cyber operations require more flexibility between offense and defense than any other form of warfare, and that cyber operations are as capable of executing a supporting role, a supported role, or an independently decisive role in war. For these reasons, cyberspace operations require consideration for equal resources to the air, land, sea, and space domains if it is truly going to be a capable military means to achieve political objectives.

Chapter 5 continues by briefly applying the proposed cyberpower targeting theory to potential US homeland threats with intent to highlight national security concerns. The potential threats drive a discussion toward organization structures, education and training, and policies which lead to the following questions: Is the US organized to fight cyber warfare? Are tax-payer dollars being wasted by multiple agencies within the US conducting similar functions? Who is the driving authority for cyber policy within the US, and under what authority is retribution for non-compliance achieved? Given the scope of this paper toward a cyberpower targeting theory, these questions are cursory in nature. Their intent is to stimulate thinking regarding potential changes in how US organizations manage critical national security infrastructure which can be manipulated by cyberspace operations of an adversary.

Beyond the Scope

It is important to address up front a few areas this thesis does not spend time discussing. The intent to develop a cyberpower targeting theory should be clear by now. However, the development of the tools to affect the targeting objectives is not the focus of this paper. In other words, for airpower, it is important to discuss whether laser guided munitions or a nuclear bomb is applicable to destroy a specified target. It is also important for the planners of an Air Tasking Order to determine what aircraft is needed to conduct a mission. This scenario carries over to the kind of support needed from intelligence planners for intelligence preparation of the battlefield, to logistical support for ensuring munitions are on-hand, to the right maintenance personnel for mission aircraft. Although these are vital, and needed for effective and efficient air operations, their focus is on the weaponry needed to support airpower toward its targeted objective. All of these same concerns exist for cyberpower and must be addressed and considered by strategists planning cyber operations. However, the author advocates all of those considerations follow the determination of a cyberpower targeting doctrine. Once the AF determines what it wants to target, whether offense, defense, or for exploitation, then it can perform all other support functions necessary to enable defined objectives; including building the weaponry required. Debates over whether electronic warfare, or the use of the electromagnetic spectrum is vital to cyberspace operations is beyond the scope as well. The author agrees with Daniel Kuehl's definition in that cyberspace includes the electromagnetic spectrum, with the caveat that *the true domain is the electromagnetic spectrum and that cyberpower is wielded through the man-made infrastructure which enables effects in that domain*.[39] This is also why the author believes the Air Force should consider combining inherent electronic warfare capabilities with Twenty-Fourth Air Force to harmonize cyberspace energies. But that, too, is beyond the scope of this treatise.

[39] Daniel Kuehls's definition of cyberspace is, "Operational use of electronic technologies and the electromagnetic spectrum to create, store, modify, exchange, and exploit information and [systems] through networked technologies." The author also believes cyberspace will be used to prevent the use of, and potentially destroy information and systems supported or controlled through cyberspace in the future as well. Kramer, Starr, and Wentz, *Cyberpower and National Security*: 28-31.

The author suggests there should be serious consideration and evaluation to cyberspace operations. If the consolidation of money, manpower, and operations is limited by antiquated paradigms or stovepipe thinking based on saving the military our fathers grew up in, then Air Force leaders are failing in their primary objective which is the defense of our great nation…not of the service we serve. This does not mean we can reduce or eliminate all duplication, and sometimes it will make sense to keep operations separate between different military services. But where it makes sense, consideration should be given to consolidate operations where excessive collaboration drives inefficiencies. Can we truly recognize today's inefficiencies without defining the cyber target of each service, DOD, and national cyber operations and the intended projection of cyberpower? We do not build a ship, a tank, an aircraft, or a satellite without a strategic objective in mind, should we manage military cyberspace through a similar lens?

Summary

Chapter 1 suggests questions for cyber strategists in today's Air Force to consider. It also recommends the focus for such strategic thinking evolve around targeting an adversary's will and capabilities to fight. Cyberpower is not limited only to activities within the realm of cyberspace itself, but rather any diplomatic, informational, military, or economic instrument of power; as well as any commercial, industrial, or other societal capability supported in, through, or from cyberspace. Simply put, from a military perspective, any land, sea, air, space, or cyber capability, that employs cyberspace in any way, has the potential for disruption by an adversary's cyberpower if left vulnerable.

By defining potential targets both of potential adversaries, as well as within the US, the Air Force can establish a trajectory to organize, train, and equip forces for offensive, defensive, and exploitation operations. Today's Air Force cyberpower traditions are similar to the "*Proficimus More Irretenti*"[40] motto of the men of the Army Air Corps in the 1920s. The possibilities are boundless, but with constrained budgets and rapidly changing technology, the Air Force must pursue specific objectives and not leave the first war initiated, and/or dominated, by cyberspace operations to chance. Looking

[40] ACTS Motto: Proficimus More Irretenti means 'We Make Progress Unhindered by Custom'. Finney and History, *History of the Air Corps Tactical School, 1920-1940*: v.

back at how early airpower advocates shaped the future of airpower might offer valuable lessons for cyberpower strategists of today.

Chapter 2

From Airpower Development to Targeting the Industrial Web

> *The Goddess of Change was turning her disturbing attention to the sky.*
> *The first great boom in aeronautics was beginning.*
>
> H.G. Wells

From the time when fictional writers spurred thoughts in children and adults alike until bombs reigned down from the sky in actual warfare, there were a plethora of possibilities as to what the invention of aerial flight would bring to warfare. Despite claims that the first military use of aerial devices came from the Chinese invention of the kite in approximately 200 BCE, and excluding balloon use in warfare, it is safe to proclaim effective military use of aviation did not occur until after the first manned aircraft flight of 1903.[1]

This chapter describes US aircraft development from infancy to use in warfare. The focus is not on the wars themselves, but rather the intended use of military airpower compared to doctrine of the time. Questioning whether technology of the time enabled objectives is relevant; as is gaining an understanding of leadership agendas and expectations for the role of airpower compared to conventional thinking of the time. What shaped these thoughts and actions? What drove changes in thinking? How was airpower enabled to achieve a dominant role in warfare as theorists such as Douhet, Trenchard, and Mitchell claimed was possible? [2] It was these theorists and the practical application of airpower in World War I that shaped doctrine and use of airpower in future wars.

Following a brief history on early rules of airpower and airpower development, we delve into the chapter's primary focus of understanding the industrial web theory as it

[1] J.G.D. Xiaoming Zhang, *Red Wings Over the Yalu: China, the Soviet Union, and the Air War in Korea* (Texas A&M University Press, 2003), 13.

[2] Giulio Douhet was an Italian airpower theorist who authored *The Command of the Air*. Douhet advocated the airplane is the offensive weapon par excellence (15) and enabled a nation to completely destroy ones enemy while protecting one's own country (23). In his general principles of aerial warfare, Douhet is also credited for advocating for an independent Air Force (49). Although Douhet gained experience in WW I regarding the use of airpower, he is known for having less concern regarding moral bombing than other airpower theorists of the day. Douhet was focused on destructing the will of the people through physical destruction of a nation, once their air force was destroyed. G. Douhet et al., *The Command of the Air* (University of Alabama Press, 2009).

relates to targeting objectives by aircraft during war and peace. How and why was this theory developed? What was its focus? How did it affect US airpower doctrine, strategic thinking, and operations within the Army Air Corps of the day? Did the focus on strategic bombing of vital centers aide technology development while blinding senior leaders of airpower limitations of the day? A case study of World War II will round out the chapter by highlighting relevant aspects of airpower abilities and limitations during these early years and how it set the framework for strategic targeting in the future.

International Rules: Fear of Airpower

By 1899 a pervasive attitude that balloons "will be used to drop explosive substances" led to an international agreement and "five-year ban inhibiting a projectile or explosion from a balloon."[3] However, this prohibition did not prevent military tacticians of the day from considering the possibilities of aerial warfare during the time of the ban. What it may have done was slowed the technological development of weapon systems and potentially limited the thinking about roles and missions for airpower in the next major war; World War I.

The 1899 ban expired and it was not until three years after World War I that the rules were updated. However, the "Hague Draft Rules of 1923 provided no definitive guidance or international law" regarding targets for bombing by airpower.[4] Although not adopted, the draft rules did serve as an example of customary international law, whereby, nations observe the rules of custom, rather than a formal convention. As international law evolved, so too did airpower strategy. From early twentieth century theorists, to fictional writers focused on heightening awareness, to limited experiences of airpower in warfare, each had their role in shaping airpower thinking toward future conflict. For the US, it was a group of men at the Army Air Force Air Corps Tactical School (ACTS) who

[3] The Hague, 29 July 1989, http://www.icrc.org/ihl nsf/FULL/160?OpenDocument.
[4] T.D. Biddle, *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas about Strategic Bombing, 1914-1945* (Princeton University Press, 2004), 181. For more details relevant to ban that was in effect from 1900-1905, see ICRC. You will also find the Hague Declaration XIV was adopted Declaration (XIV) Prohibiting the Discharge of Projectiles and Explosives from Balloons. The Hague, 18 October 1907 was ratified b the US and UK, but not France, Italy, Germany, or Russia. The Declaration went into effect in 1909 and was supposed to be replaced at the Third Peace Conference, however, the conference never met and it is argued that this declaration is still in effect. See ICRC, "The International Law – Treaties and Documents," 18 October 1907, http://www.icrc.org/ihl nsf/FULL/245?OpenDocument.

shaped early US airpower strategy. Theorists such as Douhet, Trenchard, and Mitchell who, as evidenced by their writings, were deeply affected by their experiences from World War I, shaped the thinking about airpower at the ACTS. The result of ACTS was a daylight bombing strategy that guided the application of US airpower in future wars.

Shaping of Strategic Bombing Doctrine

Strategic bombing found its roots in the perceived psychological impacts bombing a city would create. Although mostly exaggerated rhetoric given the primitive bombing technology of the day, the ambition is not unfounded. In 1849, during an Italian revolt against the Austrian Hapsburgs, Venice was bombed from air by projectiles carried by small linen and paper balloons.[5] These attacks were rudimentary in nature, but effective as propaganda about the 'frightful effects' of the new weapons. After manned aerial flight started in 1903, exaggerations regarding airpowers potential expanded by means of fictional writers like H.G. Wells, the author of this chapter's opening quote. Also French newspapers publishing's of how French bombing would obliterate Berlin heightened airpower awareness.[6] Additionally, airpower advocacy gained importance after the small wars in Libya during 1911-1912, and when the French put down the uprising of Morocco in 1912.[7] It would not be long before political representatives raised national concerns regarding airpower devastation through publications of their own.

Years before World War I, a British Parliamentarian named E. Joynson Hicks published an article in the National Review called "Command of the Air."[8] Aside from confirming for British citizens that bombs and bullets could in fact be delivered from airplanes, he went on to lay out a strategic role for the bomber.[9] Hicks stated bombers would target material resources to deprive their use, strike at "nerve centers," government buildings, railways, stock exchange, and attack the population itself to affect morale of the people.[10] Thus began foundations of a strategic bomber doctrine that the Royal Air

[5] Biddle, *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas about Strategic Bombing, 1914-1945*: 19.
[6] Kennett, *The First Air War: 1914-1918*: 42.
[7] Kennett, *The First Air War: 1914-1918*: 17.
[8] Kennett, *The First Air War: 1914-1918*: 43.
[9] Kennett, *The First Air War: 1914-1918*: 44.
[10] W.J. Hicks, *The Command of the Air* (Nisbet, 1916), 353.

Force (RAF) would employ in various forms in future wars. In reality, the strategic bombing strategy Hicks advocated was not limited to the RAF.

Early in 1915, during World War I, the French had over 120 aircraft prosecuting long-distance attacks on German industrial sites determined as vital to German war efforts.[11] The intent of the bombers was similar to what Hicks of Britain advocated in reducing the adversary's material resources for war. Although French bombers executed attacks on vital German centers, the French bombing theory of the day stated air forces were to cooperate with ground forces, eroding the enemy's will and capabilities.[12] This relegated the potential capabilities of airpower throughout the war and limited airpower's potential. The US Army Air Corps would experience the same challenge.

In executing air warfare in World War I, the French received help from the Royal Flying Corps (RFC) of Britain in 1914 and beyond. Whether following the recommendations of Joynson Hicks, or of his own accord, Hugh Trenchard of the RFC employed airpower to meet objectives he determined would have an effect on the adversary's abilities to wage war. Notice the subtle change between Hick's focus on morale and will, and Trenchard's focus on the capabilities to wage war. Trenchard's actions had great influence on British airpower and its history after the war.[13]

During the Somme campaign, Trenchard directed RFC pilots to fight offensive air battles in order to win maneuver for British reconnaissance, artillery, and other ground support aircraft—while denying enemy freedom to do the same.[14] Trenchard used his experiences from World War I to opine the airplane as an offensive and not a defensive weapon. Thus airpower became what Hicks advocated and a new foundational body of British air theory existed for use during and after the war.[15] These theories extended to US airpower thinking as well.

[11] Biddle, *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas about Strategic Bombing, 1914-1945*: 25.
[12] Biddle, *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas about Strategic Bombing, 1914-1945*: 25.
[13] Biddle, *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas about Strategic Bombing, 1914-1945*: 26.
[14] Biddle, *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas about Strategic Bombing, 1914-1945*: 27.
[15] Biddle, *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas about Strategic Bombing, 1914-1945*: 29.

American airpower prior to its entry into World War I in 1917 did not have first-hand experience of long-range bombing.[16] Although the Wright brothers were the first documented powered, heavier-than-air, manned-flight, the United States took a leisurely approach to developing and exploiting military applications of aircraft. By 1907 the US Army established an Aeronautical Division within the Signal Corps, but by 1911 this corps only had one aircraft and one pilot.[17] Besides the minimal force structure, the doctrine for aircraft employment was minimal in defining expected roles of aircraft in military operations. The US War Department's *Field Service Regulations of 1914* stated aviation was for reconnaissance and observation of artillery fire and by 1916 aviation was still bound to ground troops.[18]

In April 1917, Colonel William (Billy) Mitchell arrived in Europe where he would begin his advocacy for airpower and go on to become the most influential American aviator of the war.[19] After being promoted to Brigadier General and appointed Chief of Air Service, Army Group, Mitchell advocated for aviation to become a separate branch like infantry and artillery, arguing aviation will have a greater influence on the ultimate decision of war than any other military arm.[20]

Collectively the major allies of World War I—British, French, and Americans—established and attempted to exercise certain principles for the employment of airpower; aerial superiority as a prerequisite to successful air operations, a determined offensive against hostile forces to gain and maintain control of the air, focused air attacks on enemy rear positions to reduce enemy air attacks on front line friendly forces, limiting air

[16] Biddle, *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas about Strategic Bombing, 1914-1945*: 49.

[17] On 10 February 1908, Captain Chae S. Wallace of the Signal Corps, United States Army, entered into an agreement with the Wright Brothers to buy "one heavier-than-air flying machine, in accordance with Signal Corps Specifications No. 486, dated 23 December 1907." The plane was to be delivered before 28 August 1908. "Signal Corps Specification, No. 486," Air Force Historical Research Center, Maxwell Air Force Base, AL., file 167.6-1, IRIS 1012791 (1907-1940), (accessed 15 April 2013).

[18] Biddle, *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas about Strategic Bombing, 1914-1945*: 49.

[19] A.F. Hurley, *Billy Mitchell, Crusader for Air Power* (Indiana University Press, 1975), 2.

[20] Benjamin Foulois was personally requested by General Pershing to assume the duties of Chief of the Air Service, American Expeditionary Force (AEF) in November 1917. General Foulois, however, recommended Billy Mitchell for the job of leading combat air efforts as Chief of the Air Service, First Army. J.S.S. OFFICE OF AIR FORCE HISTORY WASHINGTON DC, *Foulois and the U.S. Army Air Corps: 1931-1935* (DIANE Publishing), 10-11. Mitchell's argument for aviation to become "a single department of aviation" occurred throughout 1919 in multiple congressional committees. R.F. Futrell, *Ideas concepts doctrine : basic thinking in the United States Air Force* (DIANE Publishing, 1971), 32.

services to reconnaissance and observation failed to utilize aircraft fully, and the air arm is more effective under a single commander.[21]

Analysis of Airpower in World War I

According to Royal Air Force (RAF) history, the airplane's role in the First World War was reconnaissance, however, later uses were consequences of purposes and logic of events.[22] In other words, aviators found useful war applications for airpower when situations arose. Major General Benjamin Foulois told interviewers, "We always had ideas about using the airplanes as offensive weapons, which was contrary, of course, to military policy at the time."[23] This highlights on-going attempts by operators at the tactical level to use innovation to solve operational challenges. Once operators find tactics, techniques, and procedures that work, especially in warfare when life and death situations occur, Airmen will institute new actions as standard procedure even though current doctrine or policy may not reflect the action.

Following the war, despite airplanes being employed as "little more than [an] extension of existing weapons," it was evident to warfighters the character of war had changed.[24] "The potential application of military force through mass employment of aircraft was recognized in World War I."[25] Acknowledging this change, the Congress enacted the Army Reorganization Act of 1920, thus creating the Air Service as a combat arm within the Army.[26]

The need to train officers in military aircraft employment was a first action sought by leadership of the new Air Service, thus the Air Service Field Officers' School was activated at Langley Field in 1920. The school changed names to become the Air Service Tactical School in 1922, then the Air Corps Tactical School (ACTS) in 1926 when it

[21] Finney and History, *History of the Air Corps Tactical School, 1920-1940,* 4.

[22] W.A. Raleigh and H.A. Jones, *The War in the Air: Being the Story of the Part Played in the Great War by the Royal Air Force* (Clarendon Press, 1922), 213.

[23] Transcript of oral history interview with Major General Benjamin Foulois, December 9, 1965, U.S.A.F.H.R.C, Maxwell AFB, p. 43 as quoted in Lee Kennett, *The First Air War,* 41.

[24] A.P. De Seversky, *Victory through air power* (Simon and Schuster, 1942), 29.

[25] See collection of Hansell's military career from 1933 to 1955. Found at the USAF Historical Research Library on Microfilm. MICFILM 34142, Jan 1 1929-Jan 1 1964, Series 3, Box 4, Folder 1, Speech 5, "Development of the U.S. Air Forces Philosophy of Air Warfare prior to our entry into World War II", 1.

[26] Finney and History, *History of the Air Corps Tactical School, 1920-1940*, 7.

moved from Langley Field to Maxwell Field, Alabama.[27] Despite the name changes, the objectives of the school were the same following World War I, train air officers in the strategy, tactics, and techniques of airpower.[28]

ACTS and the Industrial Web Theory

The Air Service was not only the newest combat arm of the Army responsible for developing training and educating officers in the newest warfare domain, it had no airpower doctrinal history to use as a foundation for the Air Corps Tactical School (ACTS) course. Therefore the school focused on educating and training air officers, as well as developing air doctrine.[29]

Prior to 1926, military doctrine focused on surface engagements. The Air Corps issued its first doctrine which appeared as a Training Regulation (TR) 440-15, *Fundamental Principles for the Employment of the Air Service*, on 26 January, 1926.[30] The gist of this doctrine was that Airmen aided ground forces to gain success, while acknowledging there may be special needs that take air forces away from ground forces.[31] Despite revisions, in essence this doctrine remained the same until 1940. But this did not deter airpower activists from exploring the boundaries of possibilities of airpower's use.

Between 1926 and 1933, practitioners of airpower realized an air force enabled commanders to strike more quickly and decisively at an enemy's bases and centers of concentration.[32] This line of thinking prevailed and instruction at ACTS stated the air force objectives should be focused on destroying the enemy's military strength in the areas of: hostile air force, troops, supplies, and lines of communication in the combat zone; concentration centers and lines of communication in the communication zone; and industrial and transportation centers in the Zone of Interior.[33]

[27] Finney and History, *History of the Air Corps Tactical School, 1920-1940*, v.
[28] Finney and History, *History of the Air Corps Tactical School, 1920-1940*, v.
[29] Finney and History, *History of the Air Corps Tactical School, 1920-1940*, v.
[30] James A. Mowbray, "Air Force Doctrine Problems: 1926–Present," *Airpower Journal*, 9, no. 4 (winter 1995): 2.
[31] James A. Mowbray, "Air Force Doctrine Problems: 1926–Present," *Airpower Journal*, 9, no. 4 (winter 1995): 2.
[32] Finney and History, *History of the Air Corps Tactical School, 1920-1940*, 63.
[33] Finney and History, *History of the Air Corps Tactical School, 1920-1940*, 63.

As training and doctrine advanced through ACTS courses of instruction, thinking of the air officers continued to expand. In 1933, a movement beyond the thinking of pursuit aircraft—fighter aircraft in today's lexicon—and more toward bomber aircraft surfaced. Major Donald Wilson, ACTS course instructor, is one of the first instructors credited with preparing a course of instruction focused on attacking grounded hostile aircraft.[34] This line of thinking drove to defining targets within the interior of an enemy's country as bomber objectives; whose destruction would disrupt the entire fabric of an enemy's economy and thereby disrupt the normal day-to-day function of society.[35]

From 1935-1940, the ACTS continued to refine their targeting focus by studying the American industrial structure to determine geographic centralization of industry, the component parts of industry, the importance of various parts, and the vulnerability to air attacks. The result of this research came to be known as the Industrial Web Theory; or the targeting objectives of strategic bombing as determined by ACTS.

Up to this point in history, US military doctrine was "set forth in the Field Service Regulations of 1923" and focused on destruction of the enemy's armed forces.[36] The ACTS recognized that in the past, "except in unusual circumstances, an enemy's capital, commerce, industrial centers, or resources had not been considered proper military objectives."[37] ACTS determined the limited military objectives were due to limited military power of the day. However, with the advent of airpower, and the ability to operate in the third dimension, an entire population of a belligerent country could be targeted. "In short, using airpower to strike vital points of a nation's structure…[were] a means of achieving the military objective with the least possible cost."[38] Moving away from targets that hinged on ground strategy warfare, Major Donald Wilson of the ACTS focused airpower on targets in the interior of an enemy's country. His intent was to identify targets that "would disrupt the entire fabric of an enemy's economy and thereby to discommode the civilian population in its normal day-to-day existence and to break its faith in the military establishment to such an extent that public clamor would force the

[34] Finney and History, *History of the Air Corps Tactical School, 1920-1940*, 65.
[35] Finney and History, *History of the Air Corps Tactical School, 1920-1940*, 65.
[36] Finney and History, *History of the Air Corps Tactical School, 1920-1940*, 62.
[37] Finney and History, *History of the Air Corps Tactical School, 1920-1940*, 63.
[38] Finney and History, *History of the Air Corps Tactical School, 1920-1940*, 63.

government to sue for peace."[39] Therefore, ACTS viewed transportation, steel, iron ore, and electric power complexes as air force objectives. By attacking these targets, the industrial fabric of a nation would collapse; thus the industrial web theory was born.

From a contemporary perspective, Robert Pape, in *Bombing to Win*, captures the intent of the industrial web theory. The industrial web tied in several key producers, including basic industry and its sources of raw materials, plant machinery, power supplies, and the work force. The threat that tied workers to the web was called the industrial fabric: sources of food, clothing, and utilities. Since industrial economics were thought to be fragile, it was believed that a small number of bombers could destroy the entire economic base of an enemy, wreaking havoc on both civilian welfare and an opponent's military power.[40]

With a US airpower targeting theory, created by airpower advocates and being taught in the premier airpower school, the only thing left was to put the theory to the test. However, before evaluating history to determine if the theory met its intended objectives, it is valid to ask what impacts the theory under development had on the organization, education, training, and equipping of the US armed forces? Did the hypothesized theory shape the Army Air Corps between the two World Wars and if so, how?

Organizing, Training, and Equipping: Supporting a Targeting Theory

Unlike other air forces around the world such as the Luftwaffe, which was created during the interwar years, and the RAF, which was created during World War I, the US air force did not become an independent service until after World War II.[41] A major factor contributing to the delayed US response in creating an independent air force limited military resources during the lean interwar periods. The Navy and Army were the traditional US military force providers and neither sought to create a separate Air Force. Combine that with the stated "isolation policy" of the day by policy-makers, and there is no real civilian push for the independent force either.[42] In the end, early airpower

[39] Finney and History, *History of the Air Corps Tactical School, 1920-1940,* 65.
[40] *R.A. Pape, Bombing to Win: Air Power and Coercion in War* (Cornell University Press, 1996), 63.
[41] Pape, *Bombing to Win: Air Power and Coercion in War*: 65.
[42] According to Campbell Craig, most American statesmen were quite content to limit US foreign policy. Craig, *Destroying the Village: The Prospect of Thermonuclear War in American Security Policy*: 2. The limitations personified by the US before World War II came to an official end in 1949 when Secretary

advocates got limited organizational change to support the newest warfare domain. Despite this organizational arrangement, new warfare theories developed into doctrine during the interwar years and guided the use of airpower at the onset of World War II.

Training to test the targeting theories espoused by the ACTS is summed up primarily as aspirations. Competing interests among the services, limited aircraft assets in the Army Air Force inventory, skepticism of airpower capabilities, and current Army doctrine of the day that stated air forces support ground forces, resulted in limited training opportunities with combat aircraft. For this reason, tactics, techniques, and procedures would initially be validated in the application of airpower during World War II versus US military training grounds. The belief was that Airmen will define new tactics, techniques, and procedures to meet real-world challenges in absence of effective ones when the need arises.

At the "onset of the Great Depression" and with diminishing thoughts during the interwar period that the US might go to war "with the bomber as its foremost weapon,"[43] military aviation did not drive much technological change or innovation; at least not independently within the military. "On the contrary, economic disaster encouraged Americans to see in the rapid growth of commercial aviation a rare glimmer of vitality."[44] Airlines in the US began to expand rapidly, whether commercial passenger carriers, agricultural, or postal, innovative uses abound. Together the Army and Navy aviation, alongside commercial industry subsidized by the government, grew the range and power of military aviation.[45] Technological advances led to new bombsights, the first B-10 bomber, and the four-engine B-17 bomber with a twenty-four hundred mile range.[46] It was commercial innovations such as these that made the ACTS doctrine of precision bombing possible. Without these innovations, doctrine to guide organize, train, and equip objectives would not have been a reality.

Dean Acheson completed negotiations for an Atlantic-region military alliance. The US Senate ratified the treaty on 21 July 1949, thus breaking the American isolationist tradition. R.G. Miller and P. R Miller, *To Save a City: The Berlin Airlift, 1948-1949* (Texas A&M University Press, 2008), 189-90.

[43] P.M.S. Sherry, *The Rise of American Air Power: The Creation of Armageddon* (Yale University Press, 1987), 47.

[44] Sherry, *The Rise of American Air Power: The Creation of Armageddon*: 47.

[45] Sherry, *The Rise of American Air Power: The Creation of Armageddon*: 48.

[46] Sherry, *The Rise of American Air Power: The Creation of Armageddon*: 52.

The organizing, training, and equipping of the US Army Air Corps in the interwar years was led by the doctrine ideas and initiatives created by the ACTS. It is this point that highlights the anticipated conclusion of this thesis. When targets are identified and objectives are clearly defined, then organizing, training, and equipping can follow within a descriptive model. This does not suggest that strategists and warfighting capabilities get stuck on a model, but rather meet political objectives by defining strategic targets of an adversary as a logical starting point for developing warfighting capabilities. Even when US air forces were not independent of other military forces, the potential of airpower was discussed, evaluated, taught, and built. As with any capability, the more it is tested, the more refined and capable it can become. Or, if incapable of delivering intended results, the more irrelevant and forgotten it will become. Incidentally, for the US and airpower advocates, the opportunity for validation was just around the corner with Hitler's desire for *Lebensraum* people and his desire to challenge the perceived liberalism, capitalism, and democracy of "Americanization."[47]

Case Study: Employing the Industrial Web Targeting Theory

As airpower evolved after World War I, new airpower theorists abound. Before reviewing the air war planning documents for World War II and evaluating the effectiveness of the ACTS Industrial Web Theory, it is relevant to highlight an additional airpower theorist whose prevalence increased at the start of World War II.

At the on-set of World War II, Alexander De Seversky highlighted eleven airpower principles. Although his book, *Victory Through Airpower*, was not published until 1942, its principles undoubtedly shaped thinking of airpower advocates of the day. The intent of highlighting De Seversky's principals is not intended to suggest it shaped warfare planning directly, but it does capture the intentions of airpower advocates during this time period to over-exude airpower's role. This zealotry potentially led to divisiveness between military forces rather than created harmonizing effects. Regardless of perception, De Seversky provided a consolidated list of principles that captured what airpower theorists of the day claimed as the most significant lessons of modern airpower:

[47] J.A. Tooze, *The Wages of Destruction: The Making and Breaking of the Nazi Economy* (Penguin Books, 2008), 658.

1. No land or sea operations are possible without first assuming control of the air above
2. Navies have lost their function of strategic offensive
3. The blockade of an enemy nation has become a function of airpower
4. Only airpower can defeat airpower
5. Land-based aviation is always superior to ship-borne aviation
6. The striking radius of airpower must be equal to the maximum dimensions of the theater of operations
7. In aerial warfare the factor of quality is relatively more decisive than the factor of quantity
8. Aircraft types must be specialized to fit not only the general strategy but the tactical problems of a specific campaign
9. Destruction of enemy morale from the air can be accomplished only by precision bombing
10. The principle of unity of command, long recognized on land and on sea, applies with no less force to the air
11. Airpower must have its own transport[48]

De Seversky's principles, combined with those of early airpower theorists undoubtedly shaped the use of airpower in World War II and beyond.

The US entered combat operations of World War II on December 7, 1941 after the Japanese bombing of Pearl Harbor. Up to this point, the US maintained its isolation, or neutrality policy and while not at war did achieve economic gain through the lend-lease act of 1941. It is this act that enabled the British to sustain the war efforts against Germany after France fell and the British were financially exhausted.[49] Although the US offered this program to the global market, it was allied forces that reaped the benefit of America's industrial might. During this same period, after observing Hitler's expansionist endeavors through military force, President Roosevelt and his administration took steps to transform the US into a pre-eminent military superpower while moving toward a strategy of future air war to defeat Germany with mass production of aircraft and aero-engines.[50]

Upon entering the war, the US maintained the attitude Britain had at the beginning of war; that the bomber would always get through and that high-altitude daylight bombing would be effective in targeting the industrial fabric of Axis powers.[51] Although the US changed its operations by adding fighter escorts to bombers, and its transition to night bombing raids to increase the survivability of long-range bombers, the focus here is on the efficiency of airpower targeting and its effectiveness at ending war.

[48] De Seversky, *Victory through air power*: 123-52.
[49] Tooze, *The Wages of Destruction: The Making and Breaking of the Nazi Economy*: 403.
[50] Tooze, *The Wages of Destruction: The Making and Breaking of the Nazi Economy*: 402-04.
[51] Biddle, *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas about Strategic Bombing, 1914-1945:* 163-65.

The US created a plan to meet these objectives before the US was pulled into the war; they were known as air war planning documents and authored with input from instructors at ACTS.

Air War Planning Document – 1 (AWPD-1) was the first US strategic campaign planning document for air war against Germany and Japan written before the attack on Pearl Harbor. It was authored by a Task Force comprised primarily of four officers working in General Arnold's Air War Planning Division which was less than 30-days old. Colonel George, Chief of Air War Plans Division, along with Lieutenant Colonel Kenneth Walker, Major Laurence Kuter, and Major Haywood Hansell, Jr., rounded out the planning team. All previously served either as directors or instructors at the ACTS.[52] The prevailing attitudes that the proper application of strategic bombing would destroy the enemy's will to resist pervades AWPD-1 while its planners strove to address the following air tasks:

- To conduct a sustained and unremitting Air Offensive against Germany and Italy to destroy their will and capability to continue the war and to make an invasion either unnecessary or feasible without excessive cost
- To provide air operations in defense of the Western Hemisphere
- To provide air operations in Pacific defense; to determine the nature of our operations and size of our forces needed, in conjunction with the Army and Navy, for defense of US territories
- To provide for the close and direct air support of the surface forces in the invasion of the Continent and for major land campaigns thereafter. Large tactical air forces would be required for this task, when the Army was ready for invasion
- *Calculation of total air requirements for* accomplishment of all these tasks[53]

These air tasks focused on five objectives determined by the Air War Plans Division:

1. To conduct air operations in defense of the Western Hemisphere
2. To prosecute as soon as possible, after the commencement of war, an "unremitting and sustained air offensive against Germany"
3. To support a strategic defense in the Pacific Theater
4. To provide air support for the invasion of the European Continent if that should be necessary, and to continue to conduct strategic air operations thereafter against the foundations of German military power and the German state until its collapse
5. After victory over Germany, to concentrate maximum airpower for a strategic air offensive against the home islands of Japan[54]

Following the US entry into World War II, Air War Plan Document – 42 was created from AWPD-1 and other planning documents. AWPD-42 called for the US Army Air

[52] See the Air War Planning Document, Plan – 1, "The Process," developed by the Air War Plans Division of the Air Staff at: http://www.au.af.mil/au/awc/awcgate/readings/awpd-1-jfacc/awpdproc.htm.
[53] See the Air War Planning Document, Plan – 1, "The Process," developed by the Air War Plans Division of the Air Staff at: http://www.au.af.mil/au/awc/awcgate/readings/awpd-1-jfacc/awpdproc.htm.
[54] See the Air War Planning Document, Plan – 1, "The Process," developed by the Air War Plans Division of the Air Staff at: http://www.au.af.mil/au/awc/awcgate/readings/awpd-1-jfacc/awpdproc.htm.

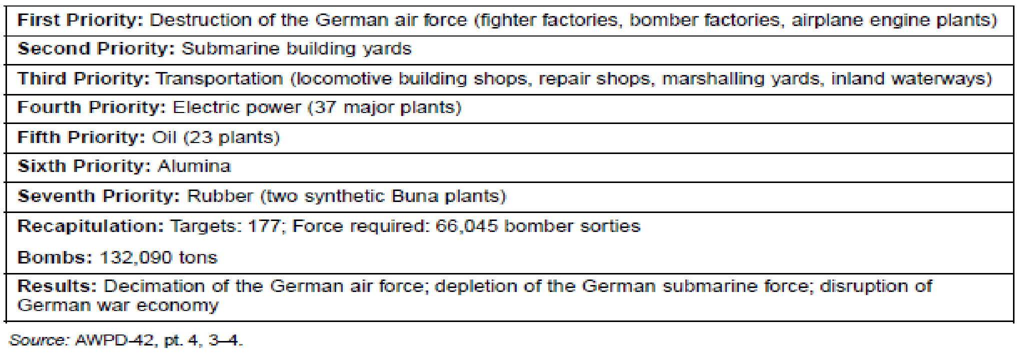
Force to concentrate on the systematic destruction of the German military and industrial machine through daylight precision bombing while RAF attacked industrial areas at night to break down morale.[55] AWPD-42 was written as a wartime production document—and as a counter to the Luftwaffe successes—after President Roosevelt requested aircraft superiority over the enemy.[56] The plan was General Arnold's response to the President's request by calling for an air offensive against Europe to deplete the German Air Force, destroy the sources of German submarine construction, and undermine the German war-making capacity.[57] The planners in the Air War Plans Division fully supported the plan despite the toned down language from AWPD-1 which advocated winning the war without an occupying force. The president's objectives appeared to fall in-line with the ACTS industrial web targeting theory.

Major Hansel believed, "that the air offensive against selected targets [in AWPD-42] should be vigorously pursued with full force for six months. The minimum effect should be a significant decline in operational effectiveness of the German army by the time the invasion of the European continent."[58] Table 1 and 2 below define initial targeting priorities of the Air War Plans Division with the intent of destroying the German's will to fight and war making capabilities.[59] Table 1 projects priorities of targeting with required equipment and armament, whereas Table 2 develops the number of targets for campaign planning.

[55] Air War Planning Document (AWPD) - 42, pt. 4, "Report," AFHRA, 145.82–42, 2.
[56] Major James R. Cody, "AWPD-42 to Instant Thunder," (Maxwell AFB, AL: School of Advanced Air Power Studies, June 1996), 13.
[57] Gen Henry Arnold memorandum to the chief of staff, subject: Combat Aircraft Which Should Be Produced in the United States in 1943, 9 September 1942, pt. 2; and "Answering Memo and Outline of Report," in AWPD-42, AFHRA, 145.82–42.
[58] H.S. Hansell, *The Air Plan That Defeated Hitler* (Arno Press, 1980), 85.
[59] Source: AWPD-42, tab B-1-a, "Air Offensive—Europe," Air Force Historical Research Agency, 145.82–42, and Major James R. Cody, "AWPD-42 to Instant Thunder," (Maxwell AFB, AL: School of Advanced Air Power Studies, June 1996), 17.

Table 1

AWPD-42 Target Priorities

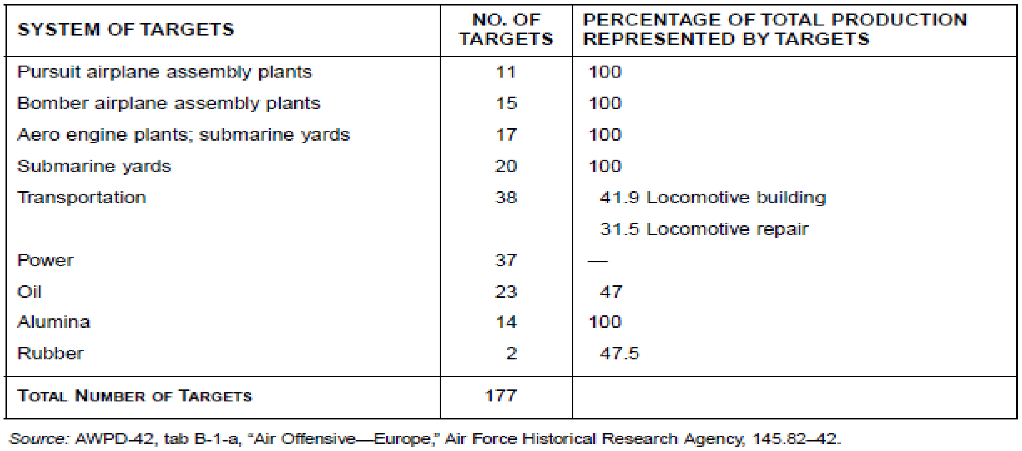


First Priority: Destruction of the German air force (fighter factories, bomber factories, airplane engine plants)
Second Priority: Submarine building yards
Third Priority: Transportation (locomotive building shops, repair shops, marshalling yards, inland waterways)
Fourth Priority: Electric power (37 major plants)
Fifth Priority: Oil (23 plants)
Sixth Priority: Alumina
Seventh Priority: Rubber (two synthetic Buna plants)
Recapitulation: Targets: 177; Force required: 66,045 bomber sorties **Bombs:** 132,090 tons
Results: Decimation of the German air force; depletion of the German submarine force; disruption of German war economy

Source: AWPD-42, pt. 4, 3–4.

Table 2

AWPD-42 Target Systems



SYSTEM OF TARGETS	NO. OF TARGETS	PERCENTAGE OF TOTAL PRODUCTION REPRESENTED BY TARGETS
Pursuit airplane assembly plants	11	100
Bomber airplane assembly plants	15	100
Aero engine plants; submarine yards	17	100
Submarine yards	20	100
Transportation	38	41.9 Locomotive building 31.5 Locomotive repair
Power	37	—
Oil	23	47
Alumina	14	100
Rubber	2	47.5
TOTAL NUMBER OF TARGETS	177	

Source: AWPD-42, tab B-1-a, "Air Offensive—Europe," Air Force Historical Research Agency, 145.82–42.

AWPD's developed by the Air War Plans Division were a first for the Army Air Corps, later named the Army Air Forces in January 1942 by Secretary of War Stimson.[60] Note in Table 1 how the targeting plan drove a required number of aircraft, 66,045 bombers to attack 177 targets; in other words targeting drove an equipment requirement. It is evident that the US war department and President Roosevelt approved AWPD-1 and AWPD-42 plans. This is evidenced both by Secretary Stimson's renaming of the Army Air Force, and the air force's expansion to a "total of 115 groups, including 34 heavy bomber groups, 12 medium bomber groups, 10 light bomber groups, 31 pursuit groups,

[60] See the Air War Planning Document, Plan – 1, "The Process," developed by the Air War Plans Division of the Air Staff at: http://www.au.af.mil/au/awc/awcgate/readings/awpd-1-jfacc/awpdproc.htm.

12 transport groups, and 16 observation groups. This expansion was a step toward the goals established in AWPD-1."[61] The relevance of airpower was becoming pervasive.

Although it would take some time for the Army Air Force to build a bomber force necessary to create the desired effects to identified targets, it was the plan for destroying identified targets that drove modest *organizational change and equipping* of the air force. It also drove the increase toward an initial 1.4 million-man draft force as the US postured itself for entry into the war. Aircrew training initiated during pre-war months and throughout the war became extremely evident by the time US efforts transitioned from Europe to the Pacific. By late 1944, US pilots had undergone over two years of training.[62] These efforts were far different than US endeavors of organizing, training, and equipping an air force for action in World War I. Without the initial will of ACTS instructors to consider the possibilities of effects of aerial targeting, then advocating for the opportunity to test these targeting theories, the senior civilian leadership may not have supported endeavors pursued in World War II.

Debates regarding the effectiveness of the bombing and the differing opinions of moral or immoral bombing of cities with area bombing versus precision bombing to achieve wars end are continually debated.[63] Although not part of this treatise plenty has been written about past wars and evaluating effects of aerial targeting. The potential effectiveness and morality concerns regarding targeting are relevant in any attempt to build a cyberpower targeting theory. These are necessary discussions which must occur

[61] See the Air War Planning Document, Plan – 1, "The Process," developed by the Air War Plans Division of the Air Staff at: http://www.au.af.mil/au/awc/awcgate/readings/awpd-1-jfacc/awpdproc.htm.
[62] M.R. Peattie, *Sunburst: The Rise of Japanese Naval Air Power, 1909-1941* (Naval Inst Press, 2007), 187.
[63] However post-war analysis is described, allied powers of Britain and the United States started the war with independent air operations against an enemy's material and moral resources. For Britain, air attacks were aimed at the sources of an enemy's strength in order to restore decisiveness to warfare and produce a much swifter and hence in the end more humane decision. As for the United States, targeting the enemy's industrial web was the focus of strategic bombers, as derived from the ACTS. Following the war, many writers criticized the strategic air campaigns against Germany and Japan; some even claimed force was employed "beyond reason." Much of the controversy centers around the ineffectiveness and inhumanity of RAF Bomber Command's avowed policy of area bombing directed against German civilian morale, the long-delayed effectiveness of US precision bombing efforts, the drift of US attacks towards a bombing of more "clublike than swordlike," and questions as to whether the immense material and human efforts devoted to bombing campaigns might have been more useful elsewhere. P. Paret, G.A. Craig, and F. Gilbert, *Makers of Modern Strategy from Machiavelli to the Nuclear Age* (Princeton University Press, 2008), 633-37.

in all realms of cyber warfare; from the possibility and planning for it, to the post-war analysis of what worked and what did not; continuous improvements must occur.

Challenges to the Industrial Web Theory

Arm chair quarterbacking frustrates the players as hindsight presents a clearer picture than looking into the unknown future. This is much like a historian writing about the past with anticipation of changing the future. Both are enjoyable from the perspective of sitting outside the sphere of execution with the ability to analyze without the penalties or pain of reality and removed from responsibility. These are the analogies for the author today while writing about targeting theories of the past. The intent of the following is not to criticize or critique but rather to acknowledge additional considerations for future theorists of warfare targeting no matter the weapon system or warfare domain of choice.

Despite different airpower theorists that advocate the will of the people or war making capabilities as strategic targets for ending war, each theory proposed finite objectives that give the appearance of static confrontation or minimal adjustments by an adversary during warfare. An example of this thinking is seen by evaluating tautology of the instructors at ACTS. After evaluating US cities, they concluded that destroying transportation, steel plants, ball-bearing manufacture, food delivery systems, energy supplies, and above all electrical power would eliminate the few vital gears whose destruction would jam vast economic systems and cause systemic disorganization.[64] Some of this rhetoric may be due to the belief that airpower was going to be so overwhelming that societies would capitulate sooner rather than later once they witnessed the destructive power of being bombed from the air. In reality, the technology needed to create the desired effects did not exist until much later in, and after, World War II. As enhanced long-range bombers, fighters, improved bomb sites, navigational aids, and ultimately the atomic bomb came to fruition, so too did the ability to achieve the devastation airpower advocates thought possible.

When evaluating strategies for war, it is relevant to think about what is possible in each warfare domain; however, it is more practical to execute what is possible given the technology and training of the day in support of established doctrine. Faber, in his

[64] Quoted in Sherry, *The Rise of American Air Power: The Creation of Armageddon*: 54.

“Competing Theories of Airpower”[65] article, highlights key questions any strategist of warfare should ask, not just advocates of airpower:

- Do you attack the source of the opponent’s power: *Sources* (military, industrial, or cultural); *Manifestations* (governmental and ideological); or *Linkages* (human and material networks)
- What targeting strategy to use: *Direct* (head-on assaults); *Indirect* (maneuver warfare); or *Rapid Transition* (Observe-Orient-Decide-Act (OODA) Loop theory of adjusting pace with an opponent)
- What level of destruction: Physical or functional destruction to degrading a system’s ability to operate leading to victory[66]

The following are the author’s interpretation of Faber’s intended message regarding warfare. Some points Faber makes, such as nation’s fight wars not just militaries, were previously known and articulated since Napoléon’s wars. But to target military entities alone within a nation to impose ones will on an adversary misses the interconnectedness of not only a nation’s instruments of power, but of the people with each of those instruments. Next are the intangibles or immeasurable attributes of warfare such as culture or ideology and how a nation’s people will react when threatened with the loss of beliefs or a way of life. Warfare is not a static constant. The enemy is a living, thinking, breathing entity with the ability to flex and change just as the US militaries believe they are. To lose sight of this basic premise in war is to forgo the lesson of Sun Tzu; “know your enemy and know yourself.”[67] Finally, before engaging in warfare a nation should know the desired outcome and plans for achieving them once victory in war is achieved. This is a critical point before war begins, when possible, as this knowledge directly contributes to either a ‘total war’ or ‘limited war’ focus for civilian and military leaders.[68] An on-going challenge for political and military leaders is to recognize the differences in these two ends of the spectrum of war. In reality, most wars will be fought somewhere within both ends. Therefore, militaries must decide which end they can organize, train, and equip toward relative to assumed risks at the time.

[65] Lt Col Peter Faber, "Competing Theories of Airpower: A Language for Analysis," paper presented at the Aerospace Power Doctrine Symposium, Maxwell AFB, Ala., 30 April 1996. This source is available on-line at http://www.au.af mil/au/awc/awcgate/au/faber htm.

[66] Lt Col Peter Faber, "Competing Theories of Airpower: A Language for Analysis," paper presented at the Aerospace Power Doctrine Symposium, Maxwell AFB, Ala., 30 April 1996. This source is available on-line at http://www.au.af mil/au/awc/awcgate/au/faber htm.

[67] Sunzi, *The Illustrated Art of War: The Definitive English Translation by Samuel B. Griffith*: 125.

[68] Limited war eludes to wars fought with “limited means for limited objectives.”Paret, Craig, and Gilbert, *Makers of Modern Strategy from Machiavelli to the Nuclear Age*: 94. Total war is explained succinctly by Clausewitz when he says, “if you want to overcome your enemy you must match the total means at his disposal and the strength of his will.” Clausewitz, Howard, and Paret, *On War*: 77. Mobilizing a nation’s full resources and society to conduct warfare against an adversary is total war.

A final thought relative to the industrial web and its seemingly specific targeting objectives. Understanding expectations and capabilities is critical to effective strategy and planning for war; as well as understanding the limitations of those expectations. It is also important to remember the need for flexibility and adaptability to changes in political objectives as those changes have the ability to directly affect the conduct of war; both from allied and adversary perspectives. When these changes occur, strategists must embrace new technology, tactics, techniques, and procedures, and innovation to meet current and future challenges. Harnessing these opportunities and not getting stuck on 'the one way' to achieve success is vital in war planning and execution; just as it is during peacetime. There is no one path to success and nothing is guaranteed to work as planned.

Summary

Table 3 below highlights early airpower theorists and their prescribed target objective of airpower.[69] It is important to recognize the infancy of airpower; its limited war tested abilities and technological capabilities, and prescribed support of ground army actions as the postulated focus of both doctrine and targeting through 1945. The works of Douhet and Trenchard were known in the US, if not directly, then indirectly through published articles of the time and limited World War I experiences. Although ACTS may not have been directly influenced by Mitchell's contributions publicly due to his courts-martial, some men who served as ACTS instructors were protégé's of Mitchell from earlier career assignments and undoubtedly incorporated his vision into airpower doctrine. The result was a growing expectation of airpower and its effects in combat. Without debating the effectiveness of World War II bombing and the fact the Army Air Force had more expectation than technical capability at the time, the targeting objectives espoused by the ACTS and the Air War Plans Division drove an air force capable of meeting wartime requirements. This was a first step toward airpower efficacy. All of these theorists, and their actions, drove initial and future organize, train, and equip

[69] This target set is a compilation of reference material reviewed in conjunction with the work of Lt Col Peter Faber, "Competing Theories of Airpower: A Language for Analysis," paper presented at the Aerospace Power Doctrine Symposium, Maxwell AFB, Ala., 30 April 1996. Available on-line at http://www.au.af mil/au/awc/awcgate/au/faber htm

functions of US air forces in some form; especially after World War II which is discussed in the next chapter.

Table 3
Early Airpower Theorists and Target Objectives

Theorist(s)	**Target(s)**
Douhet	Population (cities)
Trenchard	War materiel, transportation, communications
Mitchell	Vital centers
de Seversky	All aspects of an industrial infrastructure
ACTS	Key economic nodes (war making materials, transportation, electricity, oil)

(*Source:* "Competing Theories of Airpower: A Language for Analysis," paper presented at the Aerospace Power Doctrine Symposium, Maxwell AFB, Ala., 30 April 1996)

Chapter 3

Targeting—From Industrial Web to Warden's Rings

The key to airpower is targeting and the key to targeting is intelligence.

John A. Warden III, 1990

In *The Rise of American Airpower*, Michael Sherry quotes Hap Arnold as saying airpower's purpose is "to destroy our targets."[1] Although an oversimplification of American airpower capabilities in World War II, it highlights the strategic-level thinking and overarching military objective of early airpower advocates. One of Sherry's themes throughout his book argues early airpower leadership failed to view aerial weapons as instruments of war that kill and destroy and it is this lack of understanding which has contributed to the growth of aerial weapons and their encouraged use.[2] Was Sherry correct in his observation of airpower advocates?

This chapter disputes Sherry's claim by highlighting a contemporary airpower theorist who not only experienced aerial weapons that kill and destroy, but created an air campaign strategy to conduct airpower operations with great efficiency for killing and destruction. Sticking with the treatise focus on targeting, the objective of this review is to recognize how the air campaign planning strategies of Colonel John A. Warden III furthered airpower efficacy; while evaluating his theory for use in cyberpower targeting. Specifically, how did Warden's principles aid airpower in becoming a decisive instrument of power? Did Warden build upon targeting principals of the ACTS or develop a new targeting theory? Is there a parallel between Air Force organize, train, and equip functions and Warden's centers of gravity systems approach—5-ring model?

Airpower Targeting Evolution: Post-World War II

Korea and Vietnam are the most well-known US wars after World War II. The Cold War is another well-known war where actual combat between Soviet and American forces did not occur directly; although the two preceding conflicts are linked to the US

[1] Sherry, *The Rise of American Air Power: The Creation of Armageddon*: 237.
[2] Sherry, *The Rise of American Air Power: The Creation of Armageddon*: 361.

containment policy of the Cold War, and Soviets did support adversaries of the US on both occasions. The use of airpower conjures several questions regarding airpower targeting strategies used in both conflicts. How did airpower targeting strategy influence operations in the Korean and Vietnam War? How did these two wars influence the airpower targeting strategy used in the 1991 Operation DESERT STORM? The first portion of this chapter lays the foundation for airpower's use.

Korean War

Despite airpower limitations evidenced in World War II by the lack of precision bombing and limited technology in navigation, radar, and weaponry, American leaders, generals, and the public, entered the Korean War with inflated expectations of what airpower could accomplish.[3] Perceptions regarding airpower limitations may have been negated by airpower advancements in technology during World War II which culminated in the most advanced air weapon ever made—the atomic bomb. However, the United States Air Force entered the Korean War using the same targeting theory developed in the 1920s. Airmen hoped to achieve air superiority and gain victory by bombing economic and military targets to eliminate the enemy's capacity and will to wage war.[4]

Airpower doctrine and teaching of the day did not evolve beyond teachings of the ACTS. Major General Orville Anderson, Commandant of the Air War College in 1949, affirms the unchanged targeting strategy. He advocated, "The strategic objective of airpower is the elimination or reduction of the enemy's power and power potential. The target may be selected segments of his industrial establishment, his communications or transportation system, the source of his governmental or social control, or his military forces in being."[5] These teachings failed to capture the actual use of aerial warfare used in both the European and Pacific campaigns of World War II. Each theater employed morale bombings, which was not a part of the industrial web theory, to achieve their combat objectives. Nor did teachings advocate for simultaneous targeting of defined centers of gravity.

[3] C.C. Crane, *American airpower strategy in Korea, 1950-1953* (University Press of Kansas, 2000), 6.
[4] Crane, *American airpower strategy in Korea, 1950-1953*: 7.
[5] As referenced in the notes of Crane, *American airpower strategy in Korea, 1950-1953*: 186.. Major General Orville Anderson, "Air Warfare and Morality, *Air University Quarterly Review 2* (winter 1949): 7.

In early February, 1945, the first major American morale bombing raid in Europe was Operation Thunderclap intended to destroy Berlin and influence its citizens toward surrender.[6] In 1945, the American bombing campaign in the Pacific shifted from interdiction to attacking civilian morale through incendiary raids on urban area.[7] Despite counter-opinions regarding whether the effects of morale bombing were effective, these actions showed the US willingness to go beyond aerial targets of the industrial web theory to achieve military objectives. Robert Pape makes this point when he says, "Western publics have shrunk from using indiscriminate means against noncombatants to pressure other states."[8] However, following World War II, there is little evidence that aerial bombing focused on degrading enemy morale became part of Air Force doctrine. This is undoubtedly due to the immoral stigma attached to directly bombing civilians.

Countering published airpower doctrine of the day for strategic bombing, Bernard Brodie advocated in 1949 for the targeting of civilian morale. Brodie argues, after studying the United States Strategic Bombing Survey (USSBS) report, *The Effects of Bombing on German Morale*, World War II showed devastating attacks at a highly concentrated time could cause depressed enemy morale.[9] This was not a new concept. Early airpower zealot Giulio Douhet argued, in *The Command of the Air*, that once command of the air was achieved, air forces should keep up violent, uninterrupted action against surface objects, to the end that it may crush the material and moral resistance of the enemy.[10] Douhet posits that a battlefield will be limited only by the boundaries of nations at war, and all of their citizens will become combatants; there will be no distinction between soldiers and civilians.[11]

What airpower strategists must remember when advocating Douhetian, as well as Brodie's, principles for targeting is that political boundaries will limit airpower, or any military objective for that matter, more than doctrine or military capabilities of the day.

[6] Pape, *Bombing to Win: Air Power and Coercion in War*: 271.
[7] Pape, *Bombing to Win: Air Power and Coercion in War*: 92.
[8] Pape, *Bombing to Win: Air Power and Coercion in War*: 69.
[9] As referenced in the notes of Crane, *American airpower strategy in Korea, 1950-1953*: 188. Barry H. Steiner, Bernard Brodie and the Foundations of American Nuclear Strategy (Lawrence: University Press of Kansas, 1991), 46-64, 269 n.11; "The Morale Factor in STRAP Planning," 5 Aug 1949, Box 11, Folder 17, Papers of Bernard Brodie, Special Collections Division, University Research Library, university of California at Los Angeles.
[10] Douhet et al., *The Command of the Air*: 129.
[11] Douhet et al., *The Command of the Air*: 10.

This is especially true in limited wars such as Korea. Xiaoming Zhang, in the *Red Wings over the Yalu*, succinctly captures this point at the end of aerial conflict in the Korean War. "The air war came not to a military conclusion, but a political one. The American strategy of using aerial bombardment achieved few political or military goals despite the initial belief of many in Washington that airpower alone could defeat the enemy in Korea."[12] For this reason, military strategists must consider all potential targets and their prohibitions during warfare in order to avoid constraints while enabling airpower to achieve stated and fleeting objectives. Even if the US is prohibited from prosecuting some targets due to moral constraints, the adversary may not be constrained by the same principles. As such, thinking about the full range of potential offensive targets will highlight enemy force vulnerabilities while defining objectives for defense operations.

Between the Korean War and the next limited war in Vietnam, which was also constrained within the context of containing Communism, US civilian leadership pursued a strategy informed by the airpower targeting doctrine of the day. Although focused on nuclear targeting, the "no-cities" doctrine espoused by then Secretary of Defense McNamara highlights the US moral concern of not targeting cities directly with airpower.[13] McNamara was simply searching for a flexible nuclear response in warfare as an alternative to "Eisenhower's all or nothing military policy" of the day.[14] This counter-argument does not diminish the objective of minimizing casualties and damage caused by airpower to those forces either making war or directly supporting the war effort. The principles of controlling, restraining, and manipulating war apply to both conventional and nuclear force application in all military domains and must be considered in the newest warfighting domain of cyber as well.

Vietnam War

Political agendas and fear of war escalation constrained airpower objectives during the Vietnam War. These constraints inhibited airpower from executing targeting doctrine of the day by limiting military operations from attacking vital centers supporting war making efforts; especially early in the war. Geography drove target selection.

[12] Xiaoming Zhang, *Red Wings Over the Yalu: China, the Soviet Union, and the Air War in Korea*: 199.
[13] Craig, *Destroying the Village: The Prospect of Thermonuclear War in American Security Policy*: 157.
[14] Craig, *Destroying the Village: The Prospect of Thermonuclear War in American Security Policy*: 157.

Almost all targets picked before August 1965 were south of the 20th parallel.[15] President Johnson's personal control of the air war, as evidenced by his target list approval at the Tuesday White House luncheons, limited options for the air commanders.[16] North Vietnamese cities became "prohibited areas" for air attacks, as were airfields and surface-to-air missile (SAM) sites while under construction, to avoid provoking the Russians and Chinese from entering the war.[17] Constraints imposed on air planners drove target selection based on three objectives: the value of a target; the risk to US pilots; and the risk of widening the war.[18]

Airpower constraints waned in time as Johnson came to see the air campaign as a means to bring the North Vietnamese to the negotiating table. From the beginning of the conflict, Airman advocated a four-phase, (Table 4) ninety-four target, (Table 5) plan focused on transportation systems, oil storage facilities, and other industrial components they perceived vital to the Northern war effort.[19] After the Tet Offensive by the North Vietnamese and Viet Cong in January 1968, Johnson not only removed target restrictions from cities like Hanoi, he supported the commanding general who pressed for approval to strike targets that "might produce civilian casualties."[20] It was the Tet Offensive that caused air leaders' to diverge from their doctrinal convictions that industrial targets were the proper objectives in Vietnam. Military historian, Mark Clodfelter argues political and military controls prevented attacks against the only two targets that would have affected Northern war-making capacity: people and food.[21] The loosing of these controls freed airpower application to move beyond the industrial web targeting theory of the day.

[15] M. Clodfelter, *The Limits of Air Power: The American Bombing of North Vietnam* (University of Nebraska Press, 2006), 85.

[16] Clodfelter, *The Limits of Air Power: The American Bombing of North Vietnam*: 85.

[17] Clodfelter, *The Limits of Air Power: The American Bombing of North Vietnam*: 85.

[18] Clodfelter, *The Limits of Air Power: The American Bombing of North Vietnam*: 85.

[19] Information is derived from multiple sources: Major General Orville Anderson, "Air Warfare and Morality, *Air University Quarterly Review 2* (Winter 1949): 7, http://archive.org/details/AirPowerInThreeWars.; Robert Frank Futrell, *Ideas, Concepts, Doctrine,* vol. 2, *Basic Thinking in the United States Air Force, 1961–1984* (Maxwell AFB, Ala.: Air University Press, 1989), 259; and Clodfelter, *The Limits of Air Power: The American Bombing of North Vietnam*: 127.

[20] Clodfelter, *The Limits of Air Power: The American Bombing of North Vietnam*: 113.

[21] Clodfelter, *The Limits of Air Power: The American Bombing of North Vietnam*: 140.

Table 4

JCS Four-Phase Air Campaign Proposal

Phases	Targets	Objectives
One (3-weeks)	Lines of communication (LOC) below the 20th parallel	Reduce the flow of logistics by battering the LOCs with almost continuous attacks, and provide a clear indication to the North Vietnamese that we would increase the scope and intensity of the war if they continued their efforts to overthrow the government of South Vietnam.
Two (6-weeks)	Northeast and northwest railroads to China	By cutting these rail lines, they would be hitting the logistical system at its most vulnerable points and would be bringing the war closer to the people and the government, thereby attacking both the means and the will of the North Vietnamese to fight.
Three (2-weeks)	Ports, mine seaward approaches, ammunition, and supply areas in the Hanoi–Haiphong area	They would expect the North Vietnamese to decide that South Vietnam was no longer worth the price. By the end of phase three, most of the targets on the 94-target list would have been struck.
Four (2 weeks)	Industrial targets outside populated areas	The intent was to hit any earlier targets that had not been fully destroyed or had been repaired.
The president and secretary of defense elected only to increase the pressure on LOCs below the 20th parallel.		

Source: William W. Momyer, *Airpower in Three Wars* (Washington, D.C.: Department of the Air Force, 1978), 19.

Table 5

JCS Ninety-Four Target Scheme

Airfields
Lines of Communication
Military Installations
Industrial Installations
Armed Reconnaissance Routes
Results: End the war by employing airpower intensively against strategic targets in North Vietnam through a concentrated strategic air offensive.

Source: Robert Frank Futrell, *Concepts, Ideas, Doctrine, vol. 2, Basic Thinking in the United States Air Force, 1961–1984*(Maxwell AFB, Ala.: Air University Press, 1989), 259.

During Nixon’s Presidency, the US lost a basic necessity for a nation at war: public support. A South Vietnam spoiling operation against the Communists known as Lam Son 719 convinced the American people “that sacrifices on behalf of South Vietnamese were no longer warranted.”[22] However, shortly after taking office, Nixon assured the nation he would do whatever was necessary to safeguard American lives and honor while not abandoning the South Vietnamese.[23] For this reason, Nixon expanded the military target objectives by allowing aircraft to mine Northern ports and interdict lines of communication. His intent was to press the Communists until the Northern

[22] S.P. Randolph, *Powerful and Brutal Weapons: Nixon, Kissinger, and the Easter Offensive* (Harvard University Press, 2007), 18.

[23] Clodfelter, *The Limits of Air Power: The American Bombing of North Vietnam*: 154.

leaders agreed to release American prisoners and support an internationally supervised cease-fire.[24] Nixon's clearly defined political objectives enabled air chiefs to execute Linebacker operations with three simply stated objectives; (a) destroy war material in North Vietnam, (b) prevent the flow of war material in Vietnam, (c) interdict the flow of troops and material from the north into combat areas, South Vietnam, Laos, and Cambodia.[25]

In addition to clearly stated presidential directives, the success of Linebacker operations came from a change in Communist tactics which evolved from guerilla to more conventional, which suited Air Force bombing doctrine of the day. During the Eastern Offensive by the North, tanks and heavy artillery were effectively targeted and destroyed, as well as logistic transports intended to resupply enemy forces. Another contributor to the success of air operations in 1972 which aided Communist concessions was the delegated authority to the air chiefs to attack various targets simultaneously while controlling air operations with a single commander, both are required lessons for successful future air operations.[26] Both of these changes are evident in the post-World War I airpower theories espoused in chapter 2. Specifically, there is a "focus [of] air attacks on enemy rear positions" and placing airpower "under a single commander."[27]

Reviewing the Wars

Differences between World War II, the Korean, and Vietnam Wars can be attributed to "total" versus "limited" war objectives. In World War II, the objectives of unconditional surrender were the mandate. In both the Korean and Vietnam Wars, fear of escalation by US politicians governed war actions. The US did not want to draw the Soviets into a prolonged war and thus limited military objectives with political restrictions and prescribed rules of engagement were the order of the day. Political restrictions aside, and despite some technological innovations between World War II and the Vietnam War—long-range bombers, radar, target navigation systems, jet fighter aircraft, precision weapons, upgraded electronic warfare, and anti-radiation missiles—the

[24] Clodfelter, *The Limits of Air Power: The American Bombing of North Vietnam*: 157.
[25] Clodfelter, *The Limits of Air Power: The American Bombing of North Vietnam*: 158.
[26] Clodfelter, *The Limits of Air Power: The American Bombing of North Vietnam*: 158.
[27] Finney and History, *History of the Air Corps Tactical School, 1920-1940*, 4.

Air Force, and political leadership, failed to learn the lesson that air bombardment of the "industrial web" objectives alone could not win a war.[28]

Attacking industrial web targets along with economic, civilian, and politically sensitive targets simultaneously and continuously, without day-to-day targeting control by civilian leadership, is required for airpower to be effective. Both Korea and Vietnam showed limited war is different than total war. Adversaries fighting a guerrilla campaign in limited war are largely immune to conventional air attacks.[29] It is difficult to identify, target, and destroy the dispersed industrial web of a guerrilla force. Therefore, limited wars require a different way of thinking about warfare and strategies regarding military target objectives. Colonel John A. Warden III, a veteran Vietnam pilot, is one such thinker. He spent his career developing a contemporary targeting theory for airpower and proved its use in the limited war of Operation DESERT STORM in 1991.

The Making of a Strategist

It can be argued the advent of nuclear weapons caused a lack of critical thinking about targeting with airpower; at least at the operational and strategic levels of war. Given the destructive power of nuclear weapons, arguments for less precision bombing are viable. However, the destructive power of nuclear weapons did not abate Air Force leader's advocacy for precision strategic bombing articulated by the ACTS in the 1930s. Combat in World War II showed the bombers did not always get through, at least not without fighter escorts in highly contested environments. Neither Korea nor Vietnam changed airpower advocates beliefs "about the unprecedented decisiveness of well-targeted, well-executed bombardment attacks."[30] A derivative of this line of thinking, between the 1930's and 1990 when Iraq invaded Kuwait, was the focus on tactical airpower as evidenced by the rise of Tactical Air Command and the future Air Force Generals post-Vietnam. Then along came Warden who thought the Air Force needed to think more about strategic warfare as being *the* dominant form of warfare.[31]

[28] Randolph, *Powerful and Brutal Weapons: Nixon, Kissinger, and the Easter Offensive*: 130.
[29] Pape, *Bombing to Win: Air Power and Coercion in War*: 175.
[30] Barry D. Watts, "The Foundations of US Air Doctrine: The Problem of Friction in War," (Maxwell AFB, Ala.: Air University Press, 1984), 45-46.
[31] Major James R. Cody, "AWPD-42 to Instant Thunder," (Maxwell AFB, AL: Air University Press, 1996), School of Advanced Airpower Studies, 36.

According to Colonel Warden, airpower is constrained only by the limits placed upon it.[32] Warden developed his views from the 266 combat missions he flew in Vietnam, and his own studies of warfare. He espoused that there is no such thing as limited war, and victory could never be gained by constant cycles of concessions and escalation.[33] Although there were constant perceptions that concessions and escalations existed in Vietnam; along with rules of engagement limitations that were dictated daily by civilian leadership.

Warden's experiences and training led him to believe airpower was most effective when used as an offensive and aggressive weapon and that good tactics could not compensate for a flawed strategy.[34] Warden's interest in flawed strategies led him to think about the strategic and operational levels of war while working at the Air Staff. His interests culminated during academic studies at Texas Tech where he initiated personal studies on Grand Strategy which led to his thesis, "The Grand Alliance: Strategy and Decision."[35] It was during this time that Warden came to believe that a strategist should think in terms of paralyzing, not of killing, and should not consider the army as the only focus to achieve victory.[36] These views can be seen in a book Warden authored while at the National War College, *The Air Campaign: Planning for Combat.* Although Warden argues for three types of combat missions—air superiority, interdiction, and close air support—for air forces, it is here that we begin to see Warden's targeting theory.

Developing an Air Campaign and New Targeting Theory

In developing a strategy for air campaign planners, Warden articulates that military objectives will vary and militaries must understand these variances in order to properly affect military objectives. He suggests military objectives tend to fall into three general categories, thus developing a focus for air campaign strategists. First, military objectives can be the destruction of some or all of the enemy's forces. The importance of political objectives, as viewed by the enemy, will determine the degree of destruction of

[32] J.A. Olsen, *John Warden and the Renaissance of American Air Power* (Potomac Books Incorporated, 2007), 22.
[33] Olsen, *John Warden and the Renaissance of American Air Power*: 37.
[34] Olsen, *John Warden and the Renaissance of American Air Power*: 22-37.
[35] Olsen, *John Warden and the Renaissance of American Air Power*: 28.
[36] Olsen, *John Warden and the Renaissance of American Air Power*: 32.

enemy forces necessary by allied forces.[37] Second, the military objective can be the destruction of some or all of the enemy's economy; especially war-related economy.[38] Third, the military objective can be either the will of the government or the *will* of the people.[39] Despite historical conjectures that, "A nation is not conquered until the hearts of its women are on the ground…no matter how brave its warriors nor how strong its weapons," this last objective is the most capricious of all military objectives.[40] The *will* of a people is the most difficult to define, observe, and measure in terms of military effectiveness. With the objectives defined, Warden transitioned to what this author deems is the most critical aspect of any targeting strategy, a focus on centers of gravity.

Enemy centers of gravity can be: equipment (number of planes or missiles); logistics (the quantity and resilience of support support); geography (location and number of operational support facilities); in personnel (numbers and quality of pilots); or in command and control (importance and vulnerability).[41] Warden's early thinking on centers of gravity is focused on airpower objectives but he clearly believed the commander's most important task was to identify the centers of gravity correctly and strike them appropriately.[42] His thinking mirrors those of Clausewitz in chapter 1, "identifying the centers of gravity is the first task in planning for war."[43] To reiterate, identifying centers of gravity that will drive military targeting objectives is applicable to all warfighting domains—too include cyber.

Warden posits "targeting priorities will be a function of perceived enemy air centers of gravity."[44] Removing the word "air" from Warden's statement, it can be restated that centers of gravity determine the targeting priorities for military forces no matter the domain from which offense is conducted. A review of World War II operations makes Warden's point for both the Pacific and European theaters. While focused on axis power targets in Europe, intelligence information showed German ball bearing factories as chokepoints to military weapon manufacturing; therefore the US

[37] Warden III, *The Air Campaign: Planning for Combat*: 112.
[38] Warden III, *The Air Campaign: Planning for Combat*: 113.
[39] Warden III, *The Air Campaign: Planning for Combat*: 113.
[40] S. Hoig, P. Rosier, and A.E. Deer, *The Cheyenne* (Facts On File, Incorporated, 2009), 98.
[41] Warden III, *The Air Campaign: Planning for Combat*: 34-35.
[42] Olsen, *John Warden and the Renaissance of American Air Power*: 66.
[43] Clausewitz, Howard, and Paret, *On War*: 619.
[44] Warden III, *The Air Campaign: Planning for Combat*: 131.

targeted the factories with airpower. From an allied perspective in the Pacific, General Hansell recognized a need to have bases within 1,600 miles of Japan to attack their homeland. This made seizing bases in the Marianas a center of gravity for the US.[45] It is from his historical studies of centers of gravity that Warden developed what has become Warden's "5-ring" model.

By 1988 Warden perfected his strategic thinking in an essay called "Global Strategy Outline." In this essay he portrayed the enemy as a system with certain centers of gravity which when affected by airpower would cause an adversary to concede due to heavy cost of continuing a war.[46] Although different variances of Warden's five "Strategic Rings" model exist, the elements of them remain constant; although updated from his earlier thinking above. Table 6 and Figure 1 below depict Warden's theory.[47]

Table 6: Warden's 5-Ring Model with Objectives

	Target	**Objective**
Inner Ring	Command & Control / Leadership	Destroy the enemy's command and control from the highest civil command to appropriate level of military command
Second Ring	War Materials	Destroy enough of the enemy's war material base that he is unable to support fielded forces
Third Ring	Infrastructure	Destroy or damage enough infrastructure so that movement of goods and services becomes impossible
Fourth Ring	Population	Impose sufficient hardship on the population that the people become either unwilling or unable to support the war effort
Outer Ring	Fielded Forces	Destroy or incapacitate enough fielded forces that he is unable or unwilling to continue effective offensive or defensive operations

(Source: *John Warden and the Renaissance of American Airpower*)

[45] Warden III, *The Air Campaign: Planning for Combat*: 52.

[46] See the referenced essay in Olsen, Olsen, *John Warden and the Renaissance of American Air Power:* 108.

[47] For a post-war refined discussion by Colonel Warden regarding his centers of gravity discussion and personally expanded details of each ring of his theory, see his work titled: Employing Air Power in the Twenty-first Century, found in "Future of Air Power in the Aftermath of the Gulf War," edited by Robert Pfaltzgraff, Jr., and Richard H. Shultz, Jr., Air University Press Maxwell Air Force Base, AL., 57-82, as found in the Air University library, 358.403 F996 c2.

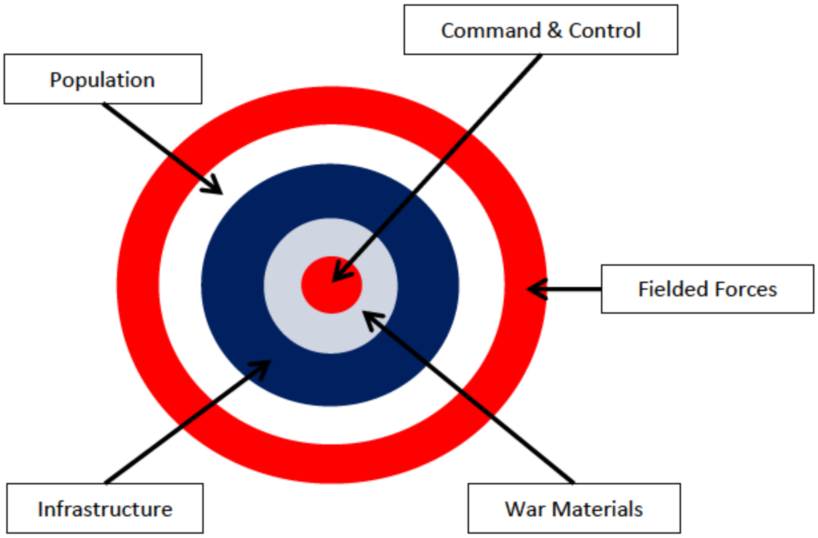


Figure 1: Warden's Five Rings
(Source: John Warden and the Renaissance of American Airpower)

Understanding the importance of a center of gravity is nothing new in warfare. During the Peloponnesian War in 431 BCE, Sparta recognized Agamemnon's navy of Athens as the strongest in the region and thus a center of gravity; just as Athens viewed Sparta's military power in the Hellas as its center of gravity. [48] Another center of gravity during the Peloponnesian War is succinctly identified by Pericles during his speech at an Athenian assembly where he encouraged Athens not give in to Sparta's requests. Pericles identified Athenian allies as a source of her power. He argued that if Athens did not march against Sparta, Athens would surely loose them.[49] Just as today, military strategies of more than 2,400 years ago had to understand and identify centers of gravity before they could determine ways to influence or destroy them in warfare.

Warden understood the history of warfare and knew he was not advocating a new principle. What he did though was create a modeling tool that included both the mechanical aspects and social aspects of a system.[50] In a mechanical analysis of his system, Warden evaluated the Soviet fuel storage capacity; something the intelligence

[48] For specifics on the strength of the Athens navy, and alliances of both Athena and Sparta, read *The Landmark Thucydides*. R.B. Strassler and V.D. Hanson, *The Landmark Thucydides: A Comprehensive Guide to the Peloponnesian War* (Simon & Schuster, 1998), 14.
[49] Strassler and Hanson, *The Landmark Thucydides: A Comprehensive Guide to the Peloponnesian War*: 83.
[50] Olsen, *John Warden and the Renaissance of American Air Power*: 116.

community deemed as not a center of gravity. Warden tested his center of gravity theory and determined that by destroying the *how* fuel was transported, and not *where* it was stored, the Soviets would run out of fuel in three to five days.[51] This changed the perspective of air planners who had concluded previously the Soviets would have six months of fuel storage in bunkers that could not be effectively destroyed. Warden's theory demonstrated that by evaluating the entire system of a capability, it became irrelevant to target every aspect of it and ultimately required less effort to affect.

Warden's model, as he postulates, is used for more than military application. For the purpose of this treatise, it portrays a targeting theory bounded by an understanding that enemy systems are integrated and reliant upon one another. It is also based on a notion that each objective has a center of gravity that supports the adversary's war making ability. In defining general targeting objectives, Warden's model focuses military attention on strategic areas required for effective air campaign plan development. This same focus applies to all warfighting domains: land, sea, air, space, and cyber.

Advancing a Targeting Model

Before evaluating the difference between the ACTS targeting theory and Warden's 5-rings, there is one amendment one could make to Warden's model. A sixth ring could be added and placed between the first and second ring, pushing the remaining elements out one level. The new second ring would be labeled *Intelligence* with an objective of either destroying or disrupting the intelligence gathering capabilities of the adversary, or influencing an enemy's intelligence with information operations as to deceive the enemy regarding friendly intentions, capabilities, and actions.

As in the opening quote of this chapter suggests, and given the reliance on accurate intelligence for decisions regarding war and execution throughout war, intelligence is a center of gravity for any nation or entity in peacetime and war. The intent is not necessarily to target intelligence briefs used by leadership for decision making; that would be a futile event. However, if key processing centers that collect, analyze, and synthesis the data is determined, those key nodes would be centers of gravity for a critical resource—intelligence.

[51] Olsen, *John Warden and the Renaissance of American Air Power*: 114-15.

Clausewitz acknowledges that “intelligence reports in war are contradictory; even more are false, and most are uncertain.”[52] He goes on to say that the difficulty of gaining “accurate recognition constitutes one of the most serious sources of friction in war.”[53] His point should not be lost on military strategists or war planners. A nation that creates unreliability or uncertainty in intelligence creates friction for the adversary. It also creates an advantage to the one causing the disruption, as long as their own is protected from the same effects. For this reason, the author argues *intelligence* is a center of gravity and is part of any strategic tool used in modeling combat operations.

While finalizing an updated enemy as a system targeting model, the author was graciously afforded a 90-minute interview with Colonel Warden who agrees with the author’s position. In discussing what enhancements might be made to the targeting model, Colonel Warden advised the second ring has undergone multiple iterations to capture Warden’s true intent and vision from a strategic perspective. From “key production” to “system essentials” to “organic essentials” the name did not clearly capture Warden’s intent. Finally, after years of continued education, refinement, and feedback, Warden updated his enemy as a systems model by calling the second targeting ring “key processes.”[54] This change succinctly captures varying elements leadership requires to conduct warfare, too include the author’s concern for key intelligence collection, processing, and distribution centers. With Colonel Warden’s approval, the updated model is referenced in Figure 2.

[52] Clausewitz, Howard, and Paret, *On War*: 117.
[53] Clausewitz, Howard, and Paret, *On War*: 117.
[54] Colonel John A. Warden III., interview by the author, Montgomery AL, 30 January 2013.

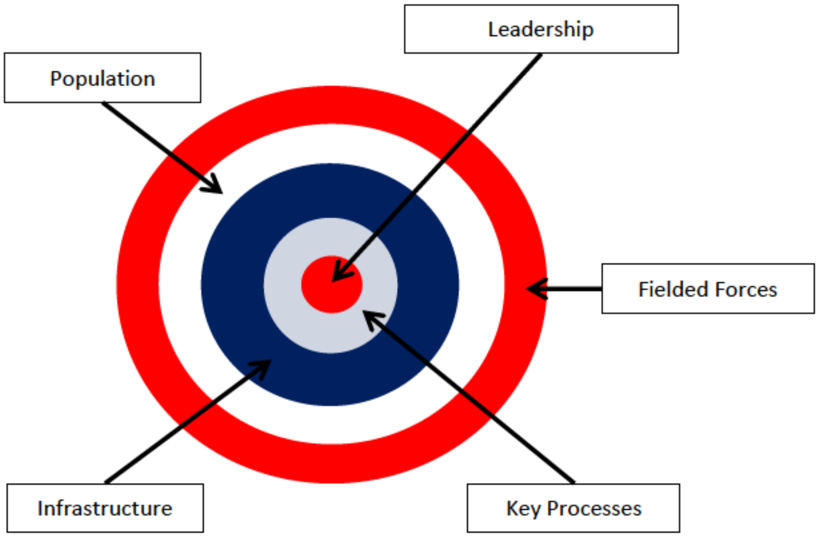


Figure 2: Warden's Updated Rings

(Source: Author's rendition per interview with Colonel John Warden)

Strategic Targeting: Moving Beyond the ACTS

Colonel Warden depicts the success of his systems targeting model when he said, "Fail[ing] to understand the shift from the physical to the function[al] obfuscate[s] analysis."[55] It also obfuscates strategic thinking. As strategists develop a theory, there must be a way to convey the theory for application, otherwise it is just a theoretical dream; and everyone knows, nightmares are dreams too. Without further digression, following through on developing a theory requires analysis once it has been applied to determine the effectiveness of the theory. The more analyzed and survivable the theory, the more widely accepted and used it becomes—at least until another revolution occurs to change the paradigm.[56]

[55] Warden III, *The Air Campaign: Planning for Combat*: 150.

[56] Thomas Kuhn defines an established paradigm as "an accepted model or pattern." Although he was specifically discussion scientific revolution and the transition between one paradigm and another, something he calls a revolution, the applicability holds with the transition from strategic bombing theorized by the ACTS to the targeting an enemy as a system of Warden. Prior to the Gulf War, airpower advocates argued for strategic bombing as the *ways* to achieve victory with airpower. Warden's model was a *revolution* in airpower thinking and proven a success in the Gulf War. Warden's theory then became the accepted model or pattern for employing airpower. T.S.A. KUHN, *The Structure of Scientific Revolutions* (University of Chicago Press, 1996), 23.

Some pundits argue Warden's theory was simply an update to "theories developed at the ACTS," as is suggested in *Warden and the Air Corps Tactical School*,"[57] This author disagrees. Warden's additions to the theory of airpower and its efficacy went beyond terminology and labels such as "vital centers." Warden drove the focus of strategic thinkers from focusing on tactical level effects of airpower up toward the operational and strategic level effects of airpower. Yes, both the ACTS and Warden espoused targets as part of a system. Both appeared to understand the inter-relation of systems when talking about specific functions such as railways providing logistics, or communications systems providing command and control. But it was Warden's targeting model that highlights how attacking disparate centers of gravity, when targeted together in simultaneous/parallel not a serial/escalatory manner, create synergistic effects upon the enemy. It was this model that enabled Airmen to show how strategic objectives could be achieved with airpower, as Warden did to the Secretary of Defense during Desert Storm.[58]

Since Warden was a literary student of Clausewitz, it is only suiting that his comparison to the studies and theories of the ACTS be equated to Clausewitz and his studies of the principles of war.[59] Military strategists agree that Clausewitz was not the first to articulate or use principles of war in battle. Understanding centers of gravity has already been mentioned above as evidenced during the Peloponnesian War. Although a center of gravity is not a principle of war, understanding that defining an objective, massing forces, use of economy of force, speed, surprise, and others to affect a center of gravity is critical to success in combat. Therefore, early practitioners of the military art

[57] Major Howard Belote, "Warden and the Air Corps Tactical School: What Goes Around Comes Around," *Air Power Journal*, (Fall 1999), http://www.airpower.au.af.mil/airchronicles/apj/apj99/fal99/belote.html

[58] In efforts to delay a ground campaign, Warden briefed Secretary Cheney about the cumulative effect of the operational air campaign. Once the brief was complete, Cheney commented, "For the first time, I understand why you people are so confident about this whole thing;" as quoted in: Olsen, *John Warden and the Renaissance of American Air Power*: 231.

[59] It is important to note that although Warden was a literary student of Clausewitz, he did not fully agree with all that Clausewitz espoused. Specifically, Warden believed Clausewitz attention on the "enemy's will" has created challenges to strategic thinking within the military. Warden's point is that the *will* of the enemy is not something military strategists can directly affect with military action. Enemy capabilities can be targeted, destroyed, or made ineffective in order to prevent the enemy from doing something friendly forces do not want to occur. Of the three broad objectives of disarming a country Clausewitz espouses, "armed forces, the country, and the enemy's will," it is the focus on the will Warden has concerns with. Colonel John A. Warden III., interview by the author, Montgomery AL, 30 January 2013.

of war must have understood the principles of war, even if they were called by a different terminology. This is exactly how Warden is compared to Clausewitz.

Clausewitz, in *On War*, is credited with combining the principles of war in a manner practitioners of war could understand and apply; as evidenced by his popularity of study in military and civilian education systems around the world. Clausewitz combination of the separate principles of war were written in such a way that they showed synergistic effects could be created by carefully planned and executed actions in war; actions which could overwhelm an adversary and cause capitulation. It highlighted the inter-connectedness of the systems used in warfare and why military tacticians and strategists should look at the enemy with a holistic approach to determine capabilities, vulnerabilities, and limitations.

On War also provides military leaders with a valuable textbook for potential success in combat; although that is presumably not what Clausewitz intended since there are no guarantees in war and the "result is never final."[60] This is precisely what Warden did. He studied the art of war, applied technical capabilities of the day, and built a targeting model based on the systems approach of the enemy centers of gravity. His model also represents a tool which can be used to plan air campaigns, and arguably a campaign in any warfighting domain, focused on achieving strategic effects in war. Finally, Warden cemented the break away from military doctrine the ACTS could not accomplish.

Although the Air Force became a separate service in 1947, there was not a war where airpower demonstrated its efficacy as it did in Desert Storm. Military doctrine during the ACTS era stated airpower provided a supporting and secondary role to ground forces as soon as air superiority was achieved.[61] Warden's advocacy showed air can perform the dominant role in combat and do it with precision. His theory's focus was designed to incapacitate the leadership and achieve functional disruption and strategic effects, rather than focus on physical destruction exhibited by strategic bombing in World

[60] Clausewitz states that even the ultimate outcome of war is not always to be regarded as final. The defeated state often considers the outcome merely as a transitory evil, for which a remedy may still be found in political conditions at a later date. It is also important to remember here that according to Clausewitz, war is the means to reach political objectives. Since political objectives may change and are not always defined in such a way that prescribes success in war, there is no political recipe for guaranteed success in combat. Clausewitz, Howard, and Paret, *On War*: 80-87.

[61] Olsen, *John Warden and the Renaissance of American Air Power*: 148.

War II. In essence, Warden's theory went beyond what the ACTS developed in thinking, understanding, and action. The case study below supports this claim.

Case Study: The Enemy as a System (5-Ring) Targeting Schema

On 8 August 1990, General Schwarzkopf phoned the Air Staff asking for a targeting plan in case Saddam Hussein committed some "heinous" act.[62] Although a preemptive action by the CENTCOM Commander, as there were no presidential directives for action against Iraq at this point, it put the wheels in motion for what would become what some consider a "new era of warfare."[63]

Timing is everything! As the deputy director for warfighting concepts, Colonel Warden had already begun to look at a "strategic" set of targets for Iraq.[64] Through analysis of how best to apply airpower in an independent fashion, and a self-directed investigation of how his core set of ideas could be applied to Iraq, Warden and his team were able to present an air campaign against Iraq the same day they received the request.[65] Built on assumptions the US would act without substantial allied support and that weapons used would cause selective damage, rather than mass aerial bombings of World War II, the air campaign was designed to limit American losses, Iraqi civilian casualties, and collateral damage.[66] There is no doubt Warden shaped these assumptions based on his knowledge of the history or warfare, as well as his experiences in Vietnam.

Warden presented a plan based on political objectives his team derived from the president's speeches, press conferences, and newspaper articles.[67] All objectives, defined in Table 7, were intended to be accomplished within six to nine days of executing the air campaign. As the table shows, the objectives Warden and his team developed for the initial air campaign plan look extensively like Warden's model in Figure 2 above. This

[62] Diane T. Putney, "From Instant Thunder to Desert Storm: Developing the Gulf War Air Campaign's Phases," *Air Power History* 41, no. 3 (Fall 1994): 40.

[63] Phillip S. Mellinger, "Ten Propositions Regarding Airpower," *Airpower Journal* 7, no. 2, (Summer 1993): 39.

[64] Diane T. Putney, "From Instant Thunder to Desert Storm: Developing the Gulf War Air Campaign's Phases," *Air Power History* 41, no. 3 (Fall 1994): 40.

[65] Olsen, *John Warden and the Renaissance of American Air Power*: 148.

[66] Olsen, *John Warden and the Renaissance of American Air Power*: 149.

[67] The military objectives derived from these resources were: withdrawal of Iraqi forces from Kuwait; restoration of Kuwaiti sovereignty; unimpeded flow of oil; and protection of American Lives. Olsen, *John Warden and the Renaissance of American Air Power*: 148.

example not only shows Warden's belief in his model, but highlights the influence his position on the Air Staff afforded him in influencing senior airpower decision makers.

Table 7: Initial Gulf War Objectives

Strategic Target	Linked to Warden's Ring	Campaign Target Objective
Leadership	Inner Ring	Two target sets: Hussein regime (isolate & incapacitate), and communications (both civil telecommunications and military command, control, and communications)
Key Production	War Materials	Four target sets: electricity, oil distribution and storage facilities, one nuclear, biological, and chemical research facility in Bagdad, and military production and storage facilities, including SCUD-related targets
Infrastructure	Infrastructure	Railroads as a target set with one railway and highway bridge as a subset
Population	Population	Three target sets: Iraqis, foreign workers, and soldiers in Kuwait (these targets were to be struck with only non-lethal, psychological weapons)
Iraqi fielded military force	Fielded Forces	Two target sets: Iraqi strategic air defense system and the Iraqi strategic offensive system (bombers & missiles). The Iraqi Army was not a target set originally.

Source: *Airpower History* 41, no. 3 (Fall 1994): 41.

Warden briefed the INSTANT THUNDER plan to General Schwarzkopf on 10 August 1990. Schwarzkopf later recalled, "I felt a hell of a lot better after I left the briefing room than when I entered it. Warden turned on the proverbial light bulb."[68] In name alone, Instant Thunder portrayed a departure from the failed Rolling Thunder of Vietnam.[69] Warden's team developed a plan intended to be quick, overwhelming, and decisive; exactly the type of "retaliation plan" the general sought.[70]

After input like General Powell's, "not being happy until he saw tanks destroyed," and other inputs received during planning briefs, Warden's team developed Instant Thunder Phase II.[71] The target sets continued to increase as airfield and naval ports were added. Before the plan was briefed to Lieutenant General Horner, the exercising CENTCOM commander in Saudi Arabia, only eighty-four targets existed on the list. Once General Horner's team took over air campaign planning the targets list grew to 481

[68] Olsen, *John Warden and the Renaissance of American Air Power*: 159.
[69] R. Hallion, *STORM OVER IRAQ PB* (Smithsonian, 1997), 143.
[70] Diane T. Putney, "From Instant Thunder to Desert Storm: Developing the Gulf War Air Campaign's Phases," *Air Power History* 41, no. 3 (Fall 1994): 42.
[71] Diane T. Putney, "From Instant Thunder to Desert Storm: Developing the Gulf War Air Campaign's Phases," *Air Power History* 41, no. 3 (Fall 1994): 42.

by early January as honed intelligence—something pre-crisis planning showed as deficient—became available.[72] Colonel Warden's targeting strategy was now in motion.

On January 16, 1991, when Baghdad went "black" forty-five seconds into the war, Warden proclaimed: "The war is over, we won."[73] Although the air war lasted longer than the six to nine days originally estimated, and despite all the convincing Warden had to do at the highest levels of the DOD to allow the air war to continue beyond those initial estimates, Warden's strategic targeting model proved accurate in the end; despite a 100-hour ground campaign by the US Army.[74]

Evaluating Success

The Gulf War Airpower Survey captures laconically the effects of Warden's targeting model in the opening sentence of its more than 400 detailed pages: "In many ways "Desert Storm" represents a watershed in history; for much of the war, it consisted entirely of the application of massive doses of airpower to the economic and bureaucratic infrastructure of Iraq and its military forces."[75] Instant Thunder provided mass, enabled air superiority through speed and surprise, and, as the airpower survey states,[76] "compared to previous wars, the bombing of core strategic targets in Iraq was remarkably precise and discriminate."[77] After more than forty years of unfulfilled promises, airpower achieved the concept of "victory through airpower," that Giulio Douhet, Billy Mitchell, and Hugh Trenchard espoused.[78] In developing a systems targeting model that enabled

[72] During discussion regarding the offensive air campaign, Phase I, a report by the Defense Technical Information Center highlights some of the challenges early intelligence communities has in providing information about Iraq and their actual capabilities and threats. See the Defense Technical Information Center review found in the Air University Library, Maxwell Air Force Base, AL under M-U 42992-167 c.1, Iris 317878, 35. Additional information is found in T.A. Keaney, E. Cohen, and Gulf War Air Power Survey Review Committee, *Gulf War Air Power Survey, Volume II: Operations and Effects and Effectiveness* (United States Dept. of Defense, 1993), 38.

[73] Olsen, *John Warden and the Renaissance of American Air Power*: 148.

[74] Olsen, *John Warden and the Renaissance of American Air Power*: 148.

[75] Keaney, Cohen, and Committee, *Gulf War Air Power Survey, Volume II: Operations and Effects and Effectiveness: 1.*

[76] For specific details on eight core strategic targets the air power survey evaluated, and the effectiveness of airpower against those targets, see: *Keaney, Cohen, and Committee, Gulf War Air Power Survey, Volume II: Operations and Effects and Effectiveness: 265-346.*

[77] Keaney, Cohen, and Committee, *Gulf War Air Power Survey, Volume II: Operations and Effects and Effectiveness:* 305.

[78] John D. Morrocco, "From Vietnam to Desert Storm," *Air Force Magazine,* 75, no. 1 (January 1992), http://www.airforcemag.com/MagazineArchive/Pages/1992/January%201992/0192storm.aspx.

victory through airpower, Warden truly measures up as a one of the prevailing contemporary airpower theorist. Therefore, it is relevant to evaluate whether or not Warden's 5-ring model changed the Air Force organize, train, and equip functions in any way.

Organizing, Training, and Equipping to a Contemporary Targeting Model

Desert Storm was unlike World War II in that the US did not have years to plan for equipping, training, and organizing forces before entering combat. Desert Storm was executed within months of Iraq's invasion of Kuwait in August 1990; therefore, the Air Force went to war with the force it had.[79] Given this perspective, and the fact that Warden's model was literally developed just months before the Gulf War, the only logical review of any organize, train, and equip (OT&E) changes is to observe improvements since lessons of the Gulf War. The author postulates a detailed evaluation of Air Force OT&E functions post-Gulf War will highlight whether or not Warden's model truly influenced changes in each functional area. This will make a great future study by other academics. For now, a brief evaluation of perceived major changes from previous wars that enabled airpower success in Desert Storm is described, along with perceived influences on future OT&E functions.

Survey Says? The Gulf War Airpower Survey says one of the crucial differences regarding organization during the conduct of the air campaign against Iraq, compared to Rolling Thunder in Vietnam, is the use of *one* individual responsible for the conduct of the campaign.[80] General Horner was the Joint Forces Air Component Commander (JFACC) and controlled inter-service and coalition air forces. As the JFACC, Horner focused the air campaign on objectives originally defined by Warden. He seized the initiative by attacking, isolating, and incapacitating the Iraqi military leadership and destroying Iraq's ability to conduct military operations.[81]

[79] Keaney, Cohen, and Committee, *Gulf War Air Power Survey, Volume II: Operations and Effects and Effectiveness*: 12.
[80] Keaney, Cohen, and Committee, *Gulf War Air Power Survey, Volume II: Operations and Effects and Effectiveness*: 39.
[81] Keaney, Cohen, and Committee, *Gulf War Air Power Survey, Volume II: Operations and Effects and Effectiveness*: 40.

By enabling a single air component commander, the management of tactical to strategic military objectives is better controlled than when multiple decision makers are involved; especially in time-sensitive environments. Competing interests over service specific objectives or priorities must be vetted; but in the end, there was only one decision maker with airpower authority and it proved successful. The fact that joint air force operations occur today with a single air component commander proves acceptance that airpower operations achieve maximum efficiency and effectiveness when a single air component commander is in charge of airpower operations.

Inefficiency existed during the Gulf War which training could have prevented. Under the actual conditions and pressures of war, human systems and organizations rarely work at optimal levels; especially at the beginning.[82] By the third day of Desert Storm, the pace of operations and the flow of intelligence created a challenge as the first two pre-planned days of air operations morphed into daily planning requirements for the Air Tasking Order and Master Attack Plan. As the Gulf War Airpower Survey shows, the complexities involved in the daily planning cycle were not clear before the war.[83] A 300% increase in cancelled operations after day two of the air campaign highlight the coordination failures. It took approximately a week before satisfactory coordination occurred and operation cancellations decreased.

Peacetime training to generate Air Tasking Orders and coordinating Master Attack Plans, at the ops tempo demanded in the early days of the Gulf War, presumably did not exist. At the highest monthly rate in Vietnam, 4,000 sorties were being flown each month. Compared to the approximate 100,000 sorties flown in the five-week Gulf War, it is safe to proclaim that joint and coalition forces had not experienced, nor trained to, that level of air tempo in the past four decades.[84] However, this is exactly the tempo principles of war dictate. As for the number of sorties generated in such a short duration, a large force is what enables Warden's 5-ring parallel targeting system.

Without mass, simultaneous operations cannot occur and escalation of airpower is an operational consequence; which is like stepping back to Vietnam operations. To

[82] Keaney, Cohen, and Committee, *Gulf War Air Power Survey, Volume II: Operations and Effects and Effectiveness*: 161.
[83] Keaney, Cohen, and Committee, *Gulf War Air Power Survey, Volume II: Operations and Effects and Effectiveness*: 161.
[84] R. Hallion, *Storm Over Iraq: Air Power and the Gulf War* (Smithsonian Institution Press, 1992), 209-19.

prevent disorder and aid future air operations, the Air Force conducts Air Tasking Order plans and development training, and Air Operation's Center training. This training provides core fundamentals to Airmen who coordinate Air Tasking Orders and Master Attack Plan requirements. Success in the past twelve years of air operations in Iraq and Afghanistan are the fruits of this training success.

Finally, advancements in equipment enabled the successful execution of Warden's model. The author is not arguing success would not have been achieved without technological advances that occurred in stealth aircraft or precision munitions, it just would not have occurred as quickly and more ordinance would have been required.[85] The simple fact is, Desert Storm proved stealth technology enabled airpower operations to be more efficient than deploying bomber and escort fighter packages of wars past, while technology increased munitions effectiveness. The result is more targets attacked with less sorties flown than ever before.

The US pursuit to maintain the latest generation bomber and fighter aircraft and to seek continuous improvements in munitions technology and precision weaponry affirms the need for these capabilities in future wars. A result of this high-tech equipment pursuit is an inferred need of these assets to achieve decisive air superiority, interdiction, and close air support advocated by Warden.

Is the Air Force today using Warden's systems targeting model to organize, train, and equip the force to meet defined targeting objectives? This author posits the answer is *yes*. If military strategists and leaders agree, then a question arises regarding the effective use of cyberpower. Should a targeting model theory that enables system effects—either in a supporting, supported, or independent role—drive the Air Force cyber organize, train, and equip functions for cyber operations today? If so, can such a theory be developed from the concepts of the industrial web theory and Warden's targeting system previously discussed?

[85] For a sample comparison of the number of targets each aircraft could engage and the number of munitions to strike each target, review the airpower survey results. As a sample, an F-111 (Vietnam era aircraft still used in Desert Storm) required 14 Mk-82s to strike one radio station whereas an F-117 carrying two GBU-27s struck two separate targets on the same mission. See: Keaney, Cohen, and Committee, *Gulf War Air Power Survey, Volume II: Operations and Effects and Effectiveness*: 353.

Summary

The word "Intelligence" in the opening quote can have various meanings. Although Warden was referring to intelligence needed about enemy disposition and capabilities necessary for effective targeting of centers of gravity, the author argues intelligence can refer to the 'military genius' Clausewitz advocates.[86]

Military members must constantly pursue education in military history, professional military education, and personal education to continuously develop effective military strategies. Especially targeting strategies the author argues as key to military organize, train, and equip functions. Using learned skills and training through combat scenarios enables critical thinking about future in warfare with the ultimate objective of either preventing war with adversaries based on their fear of US capabilities, or ending war quickly when it does occur.

The men who made up the ACTS developed the art of aerial warfare and created foundational doctrine. Colonel Warden learned from doctrine and evaluated failures and successes to harness airpower's true potential in his 5-ring targeting model. Although tables 3 and 6 above appear similar, they are different in the foundational approach to applying airpower advocated by Warden. The strategic bombing targets promoted by the ACTS directly supported the military functions and capabilities in some manner, whereas Warden's model targeted the national strategic targets that went beyond military centers of gravity. It was not just about attacking industrial and economic targets advocated by the ACTS, there needed to be a priority for the target sets; something Warden clearly argues as critical while placing leadership at the center ring. Additionally, targets require simultaneous, unrestricted attack to achieve decisive strategic results. Escalation of warfare capabilities, like in Korea and Vietnam, reduces combined effects of weapon

[86] Although Clausewitz' argument that the commander-in-chief be a statesman, but not cease to be a general, may not appear to military leaders today, it does. The point he is making is that military leaders who supreme commanders, must understand the entire political situation in order to achieve victory and attainment of political objectives simultaneously. The difference in his writing and today is, at the time, the military leaders were also potentially statesmen when not in war. To his point of military genius, which not all military members are intended to be, otherwise it would "be very weak." Military genius is one with the qualities of experience and observation, comprehension, and calm in war. Warden's advocacy for operational and strategic use of airpower, and his conception of the enemy as a system which could be destroyed quickly by targeting key centers of gravity, in order to achieve rapid political objectives, shows his understanding of the military as the means in achieving political ends. Clausewitz, Howard, and Paret, *On War*: 100-12.

systems and limits results derived from attacking centers of gravity simultaneously when possible. Overwhelming the enemy can be decisive and lead to quick capitulation.

Warden's military and civilian education, combined with his operational experience and an understanding of warfare, enabled him to postulate a decisive air campaign planning strategy. Although his theory was based on similar targeting principles espoused by early airpower advocates, Warden combined a priority schema with the overwhelming use of force to target objectives and create strategic effects. He was able to do this because he understood not only the capabilities of airpower, but its limitations and those imposed upon it by society as well.

Building on chapter 2, and given the limited airpower theories both created and studied beyond the ACTS and the 1930s, only Warden is considered to have made significant contributions to the thinking regarding the employment of airpower. The theorist list from chapter 2 is expanded in Table 8 below to include Warden's theory, plus a postulated addition by the author for future consideration during the development of a cyber-targeting theory in chapter 5.[87]

Table 8: Airpower Theorists & Target Objectives

Theorist(s)	Target Set(s)
Douhet	Population (cities)
Trenchard	War materiel, transportation, communications
Mitchell	Vital centers
ACTS	Key economic nodes (war making materials, transportation, electricity, oil)
de Seversky	All aspects of an industrial infrastructure
Warden **(updated)**	5 rings (Leadership, **Key Processes**, Infrastructure, Population, Fielded Military)

Source: Author based on published documents

[87] This target set is a compilation of reference material reviewed in conjunction with the work of Lt Col Peter Faber, "Competing Theories of Airpower: A Language for Analysis," paper presented at the Aerospace Power Doctrine Symposium, Maxwell AFB, Ala., 30 April 1996, http://www.au.af mil/au/awc/awcgate/au/faber htm.

It is now time to evaluate these same possibilities and limitations regarding the use of cyberpower. We will begin the next chapter by evaluating potential constraints to targeting when using cyberpower to achieve military and strategic objectives.

Chapter 4

Artifacts of Cyberpower Targeting

> *War is such a dangerous business that the mistakes which come from kindness are the very worst.*
>
> Carl von Clausewitz

> *The practice of warfare can thus be understood as the attempt to impose order over chaos, to exert control where it most threatens to elude, and to find predictability in the midst of uncertainty.*
>
> Antoine Bousquet

Considerations and challenges facing cyber warfare relative to targeting adversary capabilities is the focus of this chapter. For scoping reasons, and to avoid getting lost in vociferous discussions about the many varying concepts surrounding influences to cyber war or cyber warfare, let alone the debate of defining what constitutes cyber warfare, this chapter focuses on three specific elements—*attribution, authorities, and centers of gravity*. Although attribution, authorities, and selected centers of gravity affect the conduct of cyber warfare, this treatise does not intend to define what the US stance regarding each attribute should be, but rather posits discussion points for consideration by leadership and policy-makers alike as cyber warfare concepts evolve and is employed in war.

As the US military strives to embrace a theory of cyber warfare, practitioners should not discard known principles of warfare in the other warfighting domains—land, sea, air, and space—as current principles are just as applicable in the cyber domain. Given the lack of warfare experience in the cyber domain, academics and military advocates are left drawing logic parallels between other domains to justify on-going efforts to organize, train, and equip forces within each military service. This action is a good start as parallels will aid development by drawing upon the many lessons learned from previous warfare, no matter in what domain experience was gained. General Larry D. Welch, retired Air Force Chief of Staff, captures this point when he states, “The fundamental military objectives are essentially the same as in other domains.”[1] However,

[1] Welch, General (r) Larry, IDA Research Notes, “Challenges in Cyberspace,” Summer 2011. https://www.ida.org/upload/research%20notes/researchnotessummer2011.pdf.

as cyber warfare develops and wars occur, leadership should not inhibit new principles of warfare from developing as cyber operations evolve and experience is gained. Although the nature of war has not changed, its character continues to evolve. Cyber offers unique challenges which must be thought about, war-gamed, and standardized when possible, but it also offers greater flexibility to military commanders of tomorrow.

Principles of War for Airpower Revisited

Peering through the Air Force lens, Air Force Doctrine Document – 1 advocates unity of command, objective, offensive, mass, maneuver, and economy of force, security, surprise, simplicity, unity of effort, restraint, perseverance, and legitimacy as the principles of war.[2] These principles are intended to "serve as valuable guides to evaluate potential courses of action" and are not a "checklist to guarantee victory."[3] Since the AF is part of the joint fight it is relevant to show a correlation between service and joint doctrine.

Joint publication 3-0, *Joint Operations*, affirms every principle of war AFDD-1 does, except 'unity of effort.'[4] The point in highlighting this disparity is that although US military forces operate toward, and serve common political objectives, the services do not necessarily function with exactly the same principles of warfare. This does not change the individual services' desired *ends* of achieving the political object, but it may change the *ways* and *means* it employs to get there. This example highlights the importance of not getting stuck on tradition or beliefs, but rather suggests services are focused on the desired objectives while using available resources in proven and innovative ways. The challenge is, as it was with airpower when initially evaluated for military use, is to determine initial barriers to efficacy and work to resolve issues that prevent or delay its use in warfare. This brings us to the crux of this chapter.

[2] Air Force Doctrine Document (AFDD) - 1, *Air Force Basic Doctrine, Organization, and Command*, http://www.e-publishing.af.mil/shared/media/epubs/AFDD1.pdf, 30.
[3] Air Force Doctrine Document (AFDD) - 1, *Air Force Basic Doctrine, Organization, and Command*, http://www.e-publishing.af.mil/shared/media/epubs/AFDD1.pdf, 30.
[4] Joint Publication 3-0, *Joint Operations*, http://www.dtic mil/doctrine/new_pubs/jp3_0.pdf, I-2.

Challenges to Cyberspace

It is stated that "electronic technologies and the electromagnetic spectrum" are what make cyberspace unique.[5] The author suggests it is the estimated seven billion people in the world that make it unique.[6] The fact that cyberspace has reached the point where an increasingly wide range of social, political, economic, and military activities are dependent upon it make cyberspace both a capability and vulnerability.[7] With so much interest in what cyberspace can afford businesses, as well as individuals, and given its low cost to entry, cyberspace has truly become a tool for *virtual expansionism*. No matter what the idea, belief, news update, or economic exchange, the only limitation to using cyberspace is the innovation of mankind. For this reason, cyberspace has become a global commons.[8]

The notion of social or public good—common goods—dates back to Roman law. Roman law held that certain resources were unsuited for ownership by individuals or governments; therefore, they were distinguished as res communis, or a 'thing (res) for everyone' (communis), and res nullius, or 'thing for no one'.[9] Res communis was applied to air and sea domains as they were perceived to be used by all. More recently, space is considered a "global commons," and has support from advocates like the US who seek to "assure the use of space for all responsible parties."[10] Keeping with the view

[5] Daniel Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," as found in D.S. Reveron, *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World* (Georgetown University Press, 2012), 34.

[6] World Population as derived from open-source info at: http://en.wikipedia.org/wiki/World_population.

[7] Daniel Kuehl, "From Cyberspace to Cyberpower: Defining the Problem," as found in Reveron, *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*: 34.

[8] The term 'global commons,' as used by the author, relates to the freedom to use the electromagnetic spectrum in order to conduct cyberspace activities. Although man-made technology that enables cyberspace operations may be controlled by geographical boundaries and nation-state rules, it is the electromagnetic spectrum that is *res communis*. A challenge from an international perspective is defining what part of cyberspace (the collective electromagnetic spectrum and technology to use cyberspace) is res communis. Given the reliance of other domains upon cyberspace, it can be argued that other domains depend on cyberspace for increased effectiveness. "Therefore, temporary disruptions of one global common can undermine the efficiency of the others." Lorenzo Valeri, "Countering Threats in Space and Cyberspace: A Proposed Combined Approach," (Chatham House: January 2013), 2, http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/0113discussionpaper_Valeri.pdf.

[9] E.C. Dolman, *Astropolitik: Classical Geopolitics in the Space Age* (Taylor & Francis, 2001), 97.

[10] Avis Lang claims most of the world's scientists recognize space is a global common in the "Editor's Note" of N.G. Tyson and A. Lang, *Space Chronicles: Facing the Ultimate Frontier* (W. W. Norton, 2012),

that cyberspace can be used by anyone with access without detracting from others, cyberspace is res communis. But is it really?

Actions within cyberspace, in democratic societies, are primarily self-regulated up to this point in history, although some simply view cyberspace as the "Wild West" of days past.[11] The falsity of accepting cyberspace as res communis is the belief that any one person using cyberspace cannot prohibit others use of cyberspace. This is false absolutely. Without getting into the variety of ways cyberspace can be limited by actors within the domain, a quick understanding of a distributed denial of service (DDOS) attack makes the point. The intent of a DDOS attack is simply to temporarily or permanently disrupt the service between a host and the service provider. In other words, Internet communications between an individual and their action through cyberspace is reduced to extremely slow processing or blocked completely.[12]

Accepting 'The Tragedy of the Commons' as outlined by Garret Hardin, a conclusion is reached that humanity is prohibited from saving the commons through individual action.[13] Therefore, the only solution is to organize cyberspace based on bureaucratic law since self-regulation will not work.[14] Gary Hart, a former member of the Senate Armed Services Committee, suggests "establishing an international cyber-security monitoring and management agency," may help stabilize this new global common.[15] This move toward governance is not new as "signs to govern cyberspace [have] slowly emerg[ed]" within the United Nations since 2004.[16] The argument is not to say that the government should create or fully control the public good relevant to a

xiv. United States of America, *National Space Policy*, (Washington, DC: Office of the President of the United States, 28 June 2010), 3.

[11] Gregory Rattray, "An Environmental Approach to Understanding Cyberpower," in Kramer, Starr, and Wentz, *Cyberpower and National Security*: 274.

[12] Distributed denial of service attacks are an attempt to saturate a network by overwhelming its network capacity and thus limiting inbound and outbound traffic via the network. For concerns regarding DDOS filtering and an adversary's counter-actions, see Edward Amoroso, Cyber Attacks. E. Amoroso, *Cyber Attacks: Protecting National Infrastructure* (Elsevier Science, 2010), 60-61.

[13] Garret Hardin was an American ecologist who warned of the dangers of overpopulation. For an overview of Tragedy of the Commons, see Dolman, *Astropolitik: Classical Geopolitics in the Space Age*: 97-103.

[14] Dolman, *Astropolitik: Classical Geopolitics in the Space Age*: 103.

[15] Gary Hart, "After bin Laden: Security Strategy and the Global Commons," *Survival: Global Politics and Strategy*, (Vol.53 no.4, August-September 2011), 19-25, http://www.iiss.org/publications/survival/survival-2011/year-2011-issue-4/after-bin-laden-security-strategy-and-the-global-commons/.

[16] Tim Maurer, "Cyber Norm Emergence At the United Nations," (September 2011), 6, http://belfercenter.ksg harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf.

socialistic society. According to Mancur Olson in *The Logic of Collective Action*, the challenge to government involvement is that "when the government provides collective goods it restricts economic freedom; when it produces the non-collective goods usually produced by private enterprise it need not restrict economic freedom."[17] For these reasons, government involvement should focus on "separate and selective incentives" to stimulate rational individuals to act in a group-oriented way."[18] "Selective incentives can be either negative or positive," but they must focus on the actors who challenge the social norms of a global common and cannot be indiscriminate in nature.[19] Therefore, knowing who is conducting cyberspace actions is critical, especially if negative incentives are required by those authorized to conduct such action in order to shape undesired cyberspace activities. This leads to a host of questions.

Why is attribution vital to cyberspace operations? Is attribution possible in cyberspace or is it continually an Achilles Heel? Under what authority is cyberpower wielded by military force, and are rules of engagement required for those operations? Is the use of cyberpower limited to military forces? Does world globalization, as evidenced by the interconnectedness of business, economics, and societies to cyberspace, effect the wielding of cyberpower? Does cyberspace further remove the warrior from morality concerns of warfare? These are not an all-inclusive list of questions surrounding the use of cyberpower, but they are some of the front-line on-going discussions surrounding academia, society, corporations, and the military alike.

As the chapter delves into the three elements discussed above—attribution, authorities, and centers of gravity—it is important to begin from a baseline of what constitutes cyber war. Does cyber war and cyber warfare mean the same thing? Given the infancy of cyber warfare discussions, differing opinions on how to conduct cyber warfare and its potential limitations in war are good conversations to have. However, at some point, sound doctrine must be established and progressive efforts moved forward so the US and the international community alike knows the parameters of what actions within, through, or from cyberspace will constitute war with the US. Otherwise, US

[17] M. Olson, *The Logic of Collective Action: Public Goods and the Theory of Groups* (Harvard University Press, 1965), 95.
[18] Olson, *The Logic of Collective Action: Public Goods and the Theory of Groups*: 51.
[19] Olson, *The Logic of Collective Action: Public Goods and the Theory of Groups*: 51.

citizens will continue to see comments from the US national security advisor like, "[US businesses share serious concerns] about sophisticated, targeted theft of confidential business information, and proprietary technologies through cyber intrusion."[20] Then, US military forces see policy-maker comments like, "We will take action to protect our economy against cyber-threats," and wonder what type of military response is feasible.[21] A cyber-attack that does not cause visible kinetic effects seems to reduce the response threshold versus an airplane flying into a building, or an anti-satellite rocket being fired. The author's question is, why is a cyber-attack treated differently?

Knowing the definition of what constitutes cyber war and having it standardized across the US military services, along with a common understanding of what constitutes cyber warfare, will enable efficient and effective organize, train, and equip functions. It also begins to clarify what rules or policies regarding cyberspace operations need to be created, modified, or removed both in the domestic and international environment. An additional benefit of standardized definitions is the purported standardization of tactics, techniques, and procedures regarding roles and responsibilities between military and non-military cyber operating forces, which today is muddying the operational world regarding domestic and international cyberpower operations. There is an operational pause that occurs when determining who is authorized to respond to a threating cyber event. This pause must go away if the US is going to wield cyberpower the way John Boyd suggests is required to stay ahead of the enemy.[22]

Cyber War Bytes

Thucydides reminds us that fear, honor, and interests, are three strong motivators for war.[23] However, if an adversary's intentions are not known, or cannot be associated

[20] Bill Gertz, "DC to Beijing: Stand Down on Cyber," *Counter Proliferation Center*, 11 March 2013, http://freebeacon.com/d-c-to-beijing-stand-down-on-cyber/.

[21] Bill Gertz, "DC to Beijing: Stand Down on Cyber," *Counter Proliferation Center*, 11 March 2013, http://freebeacon.com/d-c-to-beijing-stand-down-on-cyber/.

[22] Without the ability to get inside the observe, orient, decide, act OODA loop of an adversary, military commanders will find it impossible to comprehend, shape, adapt to and in turn be shaped by an unfolding evolving reality that is uncertain, ever-changing, and unpredictable. For more details regarding John Boyd, see: John Boyd Compendium, "The Essence of Winning and Losing," August 2010, http://dnipogo.org/?s=essence+of+winning+and+losing.

[23] Strassler and Hanson, *The Landmark Thucydides: A Comprehensive Guide to the Peloponnesian War*: 43.

to fear, honor, or specific interests based on public information or actions, then these motivators for war are no more than psychological operations. Although there are "psychological dimensions within any element of national power," cyberpower should not be relegated to simply another means for conducting psychological operations.[24] However, cyberpower can be one more capability to shape foreign perceptions of US military capabilities which are "fundamental to strategic deterrence."[25] The challenge is, how to determine when cyber-war is occurring when a formal declaration of war is not declared; especially when pundits argue cyber-war is on-going every day.

Martin Libicki advocates that technological and organizational innovations over the last few decades have created the potential for "non-obvious warfare."[26] Such warfare types that could plausibly be conducted in non-obvious manners include: cyber warfare; space warfare; electronic warfare; drone warfare; sabotage, special operations, assassinations, and mining; proxy attacks; weapons of mass destruction; and intelligence support to combat operations.[27] With our focus on cyber-war and cyber warfare, it is incumbent upon military professionals to understand that there is more to cyber warfare than the mundane adage of hackers attacking a system to disrupt its function, corrupt its data, or render the machine inoperable with a harmful execution file. Cyberpower can influence not only warfare in cyberspace, but capabilities in all warfighting domains. However, cyber professionals must first understand what constitutes cyber war and cyber warfare before cyber warfighting capabilities can influence actions across all domains.

Precursor to Cyber War, Cyber Warfare, and Attribution

For the US military, neither cyber-war nor cyber warfare is clearly defined in open-source doctrine. The conduct of cyber warfare can and should consider the principles of war suggested above; however, what we are talking about here is the basic definition of cyber war. With dramatists like Michael Gross touting "Stuxnet is the Hiroshima of cyber-war," and attempting to draw similarities between cyber warfare and

[24] F.L. Goldstein and B.F. Findley, *Psychological Operations: Principles and Case Studies* (Air University Press, 1996), 8.

[25] Goldstein and Findley, *Psychological Operations: Principles and Case Studies*: 8.

[26] Martin Libicki, "The Specter of Non-Obvious Warfare," *Strategic Studies Quarterly* 6, no.3 (Fall 2012): 88, http://www.au.af mil/au/ssq/2012/fall/fall12.pdf.

[27] Martin Libicki, "The Specter of Non-Obvious Warfare," *Strategic Studies Quarterly* 6, no.3 (Fall 2012): 88-9, http://www.au.af.mil/au/ssq/2012/fall/fall12.pdf.

nuclear warfare, the antennas of those in the business of military defense tend to go up.[28] Although this is an over-exaggerated analogy since Hiroshima killed an estimated 130,000 people, whereas Stuxnet is not known to have killed anyone, the warning of potential damage caused by cyber-attacks like Stuxnet is valid.[29] When cyber capabilities like Stuxnet is described as "a self-directed drone: the first known virus that, released into the wild, can seek out a specific target, sabotage it, and hide both its existence and its effects until after the damage is done," it begins to sound like special military operations in action.[30] But does an attack like Stuxnet constitute cyber war? Does the destruction of another nation's centrifuge making ability, whether or not it is believed to be constructed for use in nuclear weapons, constitute war?[31] That answer depends on ones perspective on the attack. However, that discussion is left for future debate as it is outside our scope.

Cyber warfare is any act to contest or control the cyber domain in order to dominate opposing force capabilities in any or all warfighting domains, while preventing an adversary the same freedom of action. Cyber warfare is then, the *ways* and *means* available to influence friendly and adversary capabilities in, through, or from cyberspace. Cyber-war can be an independent form of limited war or in conjunction with other forms of warfare that escalate toward, or in, total war; but really this distinction is irrelevant. What is relevant is remembering that the intent of war is "to compel the enemy to do our will."[32] For the US Air Force, cyberpower, along with airpower and space-power, are all *means* to influence an adversary's will. What the Air Force cannot do is forgo the opportunity to think about, and develop, the *ways* and *means* of influencing war through cyberpower; despite arguments like those of Thomas Rid.

[28] Michael Joseph Gross, 'A Declaration of Cyber-War', *Vanity Fair*, (April 2011): 1, http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104.

[29] Michael Sherry provides a reference derived from the Committee For Compilation, *Hiroshima and Nagasaki*, 420-421, which estimated 130,000 lives were lost in Japan by the atomic bomb in Hiroshima. Sherry, *The Rise of American Air Power: The Creation of Armageddon*: 406.

[30] Michael Joseph Gross, 'A Declaration of Cyber-War', *Vanity Fair*, (April 2011): 2, http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104.

[31] The Tallinn Manual would lead one to believe the answer is 'yes'. If this is the case, are nations setting precedence by not classifying these actions as acts of aggression or acts of war accordingly. For more specifics, see: M.N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, 2013).

[32] Clausewitz, Howard, and Paret, *On War*: 75.

Aside from harshly criticizing President Obama's national security policies, Rid believes the Obama administration is making "two crucial mistakes."[33] By signing a November 2012 policy that includes offensive use of computer attack, Rid claims the Obama administration "fail[s] to realize (or chooses to ignore) that offensive capabilities in cyber security don't translate easily into defensive capabilities."[34] Rid goes on to state the administration "fail[s] to realize (or chooses to ignore) that it is far more urgent for the US to concentrate on developing the latter, rather than the former."[35] This is exactly the trap of limited thinking in cyber warfare US military strategists cannot afford to fall into. It is not one or the other, these are not mutually exclusive. Adversaries do not think in limited terms of warfare, neither should US forces. This author argues the defensive form of cyber-war is critical, but not decisive. To be decisive in war, offensive capabilities are required and must be developed so they are available when called upon. Without US policy-maker authorities to progress offensive cyber-warfare capabilities, military forces are hindered by the political constraints Rid argues for.

With a brief concept of cyber-war and cyber warfare, now modify the Stuxnet scenario presented while applying the suggestion of Michael Gross above, and presume that the Stuxnet *worm* can "exploit" a target it specifically seeks out.[36] Understanding that the worm affects the Supervisory Control and Data Acquisition (SCADA) of a system, and that the controls over a particular system could be 'owned' by someone else, the potential exists for catastrophic damage initiated by a cyber-attack. Hypothetically speaking, the catastrophe that occurred at the Sayano-Shushenskaya Hydroelectric plant in Khakassia, Russia could have been caused by a SCADA attack.[37] Given today's virtual control of command systems via cyberspace, such as the one controlling the

[33] Thomas Rid, *National Security*, "Cyber Fail: The Obama administration's lousy record on cyber security," 4 February 2013, http://www newrepublic.com/article/112314/obama-administrations-louse-record-cyber-security.
[34] Thomas Rid, *National Security*, "Cyber Fail: The Obama administration's lousy record on cyber security," 4 February 2013, http://www newrepublic.com/article/112314/obama-administrations-louse-record-cyber-security.
[35] Thomas Rid, *National Security*, "Cyber Fail: The Obama administration's lousy record on cyber security," 4 February 2013, http://www newrepublic.com/article/112314/obama-administrations-louse-record-cyber-security.
[36] Exploitation enables the use of a discovered vulnerability to be used for the purpose an adversary might have. See E. Amoroso, *Cyber Attacks: Protecting National Infrastructure* (Elsevier Science, 2010), 35.
[37] To read more about the Sayano-Shushenskaya Hydroelectric plant incident and see pictures of visual destruction, see http://en.wikipedia.org/wiki/2009_Sayano-Shushenskaya_power_station_accident.

hydroelectric plant, the potential exists for an adversary to attack an unprotected system. Given the fact that 75 people lost their lives during the Khakassia incident and the loss of expensive resources occurred, it is conceivable that cyber-attacks can have kinetic effects.

Knowing this capability exists, one has to ask the question, “Could Stuxnet cause a nuclear weapon to destruct?” What about a nuclear weapon sitting on a launch pad waiting for the final ‘execution’ command before being fired? It would be hard to imagine the potential not existing given the many known vulnerabilities within cyberspace in the open media these days; and seemingly more each week. From this oversimplified scenario of the potential threats within, through, and from cyberspace, it behooves military strategists to strive for clarity surrounding cyberpower and its use in future warfare. One of the first and potentially most detrimental tasks to any decision regarding a response from a cyber-attack is the ability to attribute who conducted an offensive action against the US, its allies, or their interests.

Attribution Need Not be 100 Percent in Cyberspace

Attribution is particularly difficult for a cyber-attack.[38] The author argues that with or without resolution of the attribution problem, war-like endeavors through cyber-attacks in cyberspace are on-going and will lead not only to cyber-war, but to war between great powers if steps are not taken now to corral these war-like activities. This opinion differs from an upcoming publication by Thomas Rid who argues cyber-attacks fall into three categories—sabotage, espionage, and subversion—but that cyber-war has not happened and is unlikely to occur in the future.[39] However, by recognizing that “economic and technological leads are likely to become more important in international politics,” and the fact that some nations are on the verge of conflict over territorial control of various islands, it is likely that war could occur in the form of other cyber-attacks like those on-going today.[40] By acknowledging and allowing instead of condemning and

[38] Martin Libicki, “The Specter of Non-Obvious Warfare,” *Strategic Studies Quarterly* 6, no. 3 (Fall 2012): 92, http://www.au.af mil/au/ssq/2012/fall/fall12.pdf.

[39] Information from the abstract of Thomas Rid, *Cyber War Will Not Take Place*, is found at http://www.amazon.com/Cyber-War-Will-Take-Place/dp/0199330638.

[40] Kenneth Waltz discusses reasons countries gain during their development by adopting technology from other countries with more advanced economics. See K.N. Waltz, *Theory of International Politics*

preventing these war-like actions, ‘custom’ is being established everyday throughout the international community which may affect future interests of US political objectives and national security.

If a nation-state is going to declare war upon another nation based on a cyber-attack, attribution for cyber-attacks must improve. Martin Libicki acknowledges that “having a good idea of *why* a state carried out a cyber-attack” is important from a strategic perspective.[41] But it is also important to know *who* did it if the attacker did not claim responsibility. Colonel Matthew Hurley rightly acknowledges cyberspace attribution of intrusions and attacks as a problem for intelligence, surveillance, and reconnaissance professionals.[42] In reality, this is a challenge to every American from the President of the US down to every individual with Internet access to the World Wide Web; whether they know they have something to lose or not. If a cyber-attack is intended to destroy, disrupt, degrade, or control an adversary’s capability through the cyber domain, or to steal corporate knowledge or the identity of an individual, the action must be attributable with a high-degree of accuracy before law enforcement or an applicable instrument of power is called upon to respond.

Retaliation without attribution is like shooting a bullet into the dark without seeing a target. It wastes resources and potentially causes unintended damage or harm. What makes attribution so difficult in cyberspace is the complexity of the Internet enhances an attacker’s ability to hide the true source of an attack. However, do nations require a one-hundred-percent attribution factor before responding to a crisis? Or can something like Mutual Assured Destruction (MAD), albeit on a less critical scale than nuclear annihilation, theoretically work as international norms are developed regarding cyber-attacks?[43] Authors of *Cyberpower and National Security* argue attribution, or the

(Waveland PressInc, 2010), 179. Also, see a brief Wikipedia overview relevant to the People’s Republic of China (PROC), known as China, claim over the Republic of China (ROC), known as Taiwan. The separation of control has existed since 1911 and continues to raise international tensions between China, Taiwan, and other international nations to this day. http://en.wikipedia.org/wiki/Taiwan,_China.

[41] M.C. Libicki, *Cyberdeterrence and Cyberwar* (RAND Corporation, 2009), 75.

[42] Colonel Matthew Hurley (USAF), “For and from Cyberspace: Conceptualizing Cyber Intelligence, Surveillance, and Reconnaissance,” *Air & Space Power Journal*, November-December 2012, 12-32, http://www.airpower.au.af mil/digital/pdf/articles/Nov-Dec-2012/F-Hurley.pdf.

[43] Mutual assured destruction (MAD) was originally developed by John von Neumann. Bernard Brodie applied it to the “strategy for a missile age” as found in B. Brodie, *STRATEGY IN THE MISSILE AGE: Theory and Applications* (National Book Network, 2007).. The MAD theory addressed the issue that short

lack of it, "does not holistically paralyze any attempt to think fruitfully about a cyber-deterrence strategy.[44] Deterrence need not be as devastating as nuclear power to still be effective. A cyber-deterrence concept may or may not focus on destroying people and property, as was the case with MAD, but rather more toward negating in more subtle ways a nation's military, industry, financial, or other socially dependent capabilities reliant upon cyberspace to function.

As improvements in new cyber forensic technology continue, experts like Dr. Kamal Jabbour acknowledge that "detecting attacks, attributing them to a source, estimating damage, and enabling response courses of action to contain the attack and limit the damage" are getting better each day.[45] Has the time come for US policy-makers to claim that if a cyber-attack is determined, within a defined percentage of tolerance, to have originated from a particular nation, an immediate response is justified? Will this type of policy aid in reducing the continually increasing number of cyber-attacks?

Since there are varying degrees of active cyber-attack responses—from stopping an attack, diverting an attack to a honey pot, or conducting direct-action against the machine conducting the attack—maybe it is time to start escalating real-time responses in efforts to reduce the overall number and intensity of attacks.[46] This response theory is similar to public law enforcement of highway speed limits as an analogy to security on the World Wide Web. When drivers on the road see posted speed limit signs, those who want to avoid a fee or confrontation with law enforcement will obey the posted speed signs. Others may risk the confrontation based on the perceived reward gained by not obeying it. Simply put, it is a cost/benefit comparison by each driver. If we presume a nation publicizes a speed limit for all its roads and on the same day announces that its police force will not enforce the laws due to other priorities, how effective do you think

of preventive war, there was no alternative to doing whatever was necessary to erase the perceived advantage of a first strike. The end result of this theory was, once a missile launch was detected, and two of three criteria for confirming the launch location was determined accurate, then an immediate response would be initiated. For details on MAD, see: W.A. McDougall, *...the Heavens and the Earth: A Political History of the Space Age* (Johns Hopkins University Press, 1997), 212.

[44] Kramer, Starr, and Wentz, *Cyberpower and National Security*: 309.

[45] Dr. Kamal Jabbour, The Science and Technology of Cyber Operations, *High Frontier* 5, no. 3, (May 2009): 15, http://www.afspc.af.mil/shared/media/document/AFD-090519-102.pdf.

[46] A honeypot is a computer, usually virtual, without any security safeguards, in other words, designed to be infected by malware or to subvert an attackers efforts. M. Bowden, *Worm: The First Digital World War* (Grove/Atlantic, 2011), 248.

the speed limits signs will be? Sure, there will be those who follow the posting for other reasons like security, safety, or morality, but in reality, it does not matter. Without an enforcement mechanism, it is a waste of resources to post the signs in the first place.

"People are more willing to follow the direction of someone they view as an authority."[47] But who is the authority for the Internet? The Internet is touted for its openness and freedom of use, not to be constrained by laws or regulations governing its use. If that is the case, comparing the above scenario with the Internet would leave users of the World Wide Web to believe the threshold of response to an illegal action conducted on-line is minimal; even if a law is in place just like a speed limit sign posted on the side of an unenforced highway.

By changing the paradigm to enable an immediate response to illegal or harmful activity, followed by technological advancement to automate responses and putting those in place to protect US national security interests, threats from cyber-attacks may decline. Public attribution is also required once the counter-attack is complete. In other words, the counter-attack response must be openly claimed by those executing it.[48]

The question then becomes, what type of response is warranted and how are unintended side effects, like shooting a bullet into the dark, prevented? Given the inter-connectedness of operations throughout the Internet, if shutting down a computer server known to be conducting cyber-attacks also shuts down the power controller for a nearby hospital, who has the authority to execute such an action? The right level of authority may be possible, if it is known the server also controls the hospital power, but what happens when that information is unknown before a counter-attack is conducted? Is the response justified?

This simple example highlights the constant challenges to cyber-operations. It is understandable that attribution is desired before a response is initiated. However, if some risk is not accepted in cases where 100 percent attribution is not known, then the current level of cyber-attacks will not only continue to remain unchecked, they will continue to grow as more societal functions migrate to operations via the Internet. For a nation like

[47] C. Hadnagy and P. Wilson, *Social Engineering: The Art of Human Hacking* (Wiley, 2010), 199.
[48] An understanding of deterrence theory, as espoused by Thomas Schelling is relevant here. Deterrence is concerned with influencing the choices that another party will make, and doing it by influencing his expectations of how we will behave. For more on deterrence theory, see Thomas Schelling. T.C. Schelling, *Arms and influence* (YALE University Press, 2008).

the US who relies immeasurably on cyberspace for societal functions as well as military operations, this continual threat and loss of national treasure through ungoverned cyberspace is unacceptable. The "free-for-all encounters of one state duel[ing] with those of another" is indicative of the Greek Dark Age (1000-800 BCE); not a period the US or the International community should strive to emulate.[49] Therefore, the question to ask is, should an offensive cyber-force, or at least an active cyber-defense force, conduct more operations in cyberspace today to counter rising threats? If the answer is yes, where should this force reside and under what authorities will they operate? Where the force should reside is beyond this treatise, although a recommendation is alluded to in chapter 5. Keeping the focus on US Air Force efforts, we now look at authorities that govern cyberspace operations.

Governing Authorities

In a statement almost two years past, Homeland Security Secretary, Janet Napolitano, acknowledged "a comprehensive international framework" to govern cyber behaviors is at "a nascent stage."[50] Research today shows defined and accepted authorities, either for domestic governance or international laws governing cyber security, is sparse at best. However, this does not mean that a "comprehensive cyber security treaty is a pipe dream," as some experts suggest.[51] What it does suggest is that rules to governing cyberspace may best be tackled one small bite at a time, instead of pursuing an overarching international policy from the outset. If cyberspace is a global commons, as is suggested, then applying governance to operations within cyberspace after societies have been using it for more than two decades will be a challenge; but not impossible.

[49] A. Ferrill, *The Origins of War: From the Stone Age to Alexander the Great* (Westview Press, 1997), 91-94.

[50] See "Remarks by Secretary Napolitano before the Joint Meeting of the OSCE Permanent Council and ASCE Forum for Security Cooperation," Department of Homeland Security news release, 1 July 2011, http://www.dhs.gov/news/2011/07/01/remarks-secretary-napolitano-joint-meeting-osce-permanent-council-and-osce-forum.

[51] See Adam Segal, Maurice Greenberg, and Matthew Waxman, "Why a Cybersecurity Treaty Is a Pipe Dream," *Council on Foreign Relations*, 27 October 2011, http://www.cfr.org/cybersecurity/why-cybersecurity-treaty-pipe-dream/p26325.

Cyberspace will be, as James Forsyth suggests, "What great powers make it."[52] This will be the case even as lesser powers, non-governmental agencies, and criminals attempt to have their voices heard through actions deemed unacceptable between nation-states.

Accepting the premise that "the current state of cyberspace and its users does not meet most conditions that encourage self-organization," and that tragedy of the cyberspace commons is inevitable in its current state, then government controls are necessary.[53] Without controls, the non-violent actions in cyberspace today—sabotage, espionage, and subversion—will continue to escalate. When the time comes that great powers are no longer willing to tolerate the non-violent cyberspace actions, the propensity for violence not only exists, it perpetuates each day cyberspace is allowed to operate ungoverned. This is especially true if one accepts the works of Kenneth Waltz.[54] Waltz states, "The evilness of men, or their improper behavior, leads to war."[55] Therefore, it is time to stop accepting violations as the norm in cyberspace and set and enforce acceptable standards while encouraging international institutions to emulate them. To do this, the US must develop domestic sovereignty regarding cyberspace.

"Domestic sovereignty refers to the ways in which internal affairs are conducted: specifically, how authority is organized within the state and how effective is the level of control these political structures exert."[56] A challenge to implementing the required level of controls is presumably caused by the lack of understanding threats from cyberspace by the average user of the domain. Timothy Sample says, "We haven't yet experienced the destruction of a national-level cyber-attack…and the assumption is there is more time."[57] From the author's perspective, time is running out rapidly.

[52] James Forsyth Jr., "What Great Powers Make It: International Order and the Logic of Cooperation in Cyberspace," *Strategic Studies Quarterly* 7, no.1, (Spring, 2013), http://www.au.af mil/au/ssq/digital/pdf/spring_13/forsyth.pdf.

[53] See Roger Hurwitz, "Depleted Trust in the Cyber Commons," *Strategic Studies Quarterly* 6, no. 3, (Fall 2012), http://www.au.af.mil/au/ssq/2012/fall/hurwitz.pdf.

[54] Kenneth Waltz is a political scientist at the University of Berkley and Columbia University. He is one of the most prominent scholars in the field of international relations. For more information on Kenneth Waltz see http://en.wikipedia.org/wiki/Kenneth_Waltz.

[55] K.N. Waltz, *Man, the State, and War: A Theoretical Analysis* (Columbia University Press, 2001), 39.

[56] See D.J. Betz and T. Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-power* (Taylor & Francis Group, 2012), 64.

[57] Timothy Sample, "Calling for a National-Level Doctrine for the Cyber Era," *Defense Systems*, 18 December 2012, http://defensesystems.com/Articles/2012/12/18/special-commentary-cyber-era-doctrine.aspx?p=1.

"Attempts to control citizens' activities through the exercise of various forms of power in cyberspace have met unsurprisingly with resistance."[58] Just last year, cyber legislation that would have offered "protection for companies willing to work with the government to help detect and stop cyber-attacks," failed to pass the Senate.[59] A question then becomes, how can the DOD protect the security and ensure effective operations of US critical infrastructure—including energy, banking and finance, transportation, communications, and the Defense Industrial Base—which all rely on cyberspace as the *DOD Strategy for Operating in Cyberspace* suggests?[60]

One method for establishing cyberspace governance, for those areas in which national security concerns outweigh all others, "is a highly regulated online environment in which national cyberspace maps onto national physical borders and mirror national norms and standards."[61] This attempt would allow each nation their own freedoms to establish rules and governance enforceable by internal regulations. This option does not forgo the need for international standards regarding acceptable behaviors in cyberspace, it only acknowledges the need to address domestic authorities first, and then recommends leadership by example just as the US has done many times before.

One main reason to argue for domestic policy and enforcement before international endeavors can be solidified is that cyber security is not the same as past US challenges. James Forsyth suggests, "The arms control regime and the World Trade Organization (WTO) are illustrative" to a potential international cyber regime.[62] Agreeing with the examples conceptually, the difference between these two and a regime to manage cyberspace is the level of access and influence upon each. Arms control was centered on nuclear deterrence. How many individuals had, or have today, access to nuclear weapons or the related technology? The World Trade Organization, and its predecessor, the General Agreement on Tariffs and Trade (GATT), "led the world toward a more service-

[58] See Betz and Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-power*: 68.
[59] See Cheryl Pellerin, "DOD Officials Cite Advances in Cyber Operations, Security," *US Department of Defense: American Forces Press Service*, 14 March 2013, http://www.defense.gov/news/newsarticle.aspx?id=119532.
[60] Department of Defense, "*DOD Strategy for Operating in Cyberspace*," July 2011, 1.
[61] See Betz and Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-power*: 71.
[62] James Forsyth Jr., "What Great Powers Make It: International Order and the Logic of Cooperation in Cyberspace," *Strategic Studies Quarterly* 7, no.1, (Spring, 2013): 105, http://www.au.af mil/au/ssq/digital/pdf/spring_13/forsyth.pdf.

oriented economy."[63] Again, a question is how many individuals actually conduct global trade or worry about fair globalization efforts throughout society? Any change to cyberspace control mechanisms theoretically impacts every individual with access to the domain. For this reason, there are many more voices to listen to when trying to establish a regime intended to minimize cyber-security threats. This is also why examples of past regimes, like arms control or the WTO, may be a good starting point for regime discussions, but should not prescribe the initial solution. Because cyberspace is such a dynamic environment, it may be wise to pursue domestic authorities first, and then expand to international standards based on experience and leadership gained from the initiative.

For the US to pursue a path of domestic cyberspace governance, the rhetoric that USCYBERCOM is the defender of critical national cyberspace infrastructure has to stop. Otherwise policy-makers must give USCYBERCOM full lines of responsibility with applicable authority to mandate security practices, standards, and enforcement mechanisms to ensure compliance. This does not currently exist within USCYBERCOM. With upwards of "90% of the relevant infrastructure owned by the private sector," DOD does not control the majority of the US cyberspace.[64] "Cyber threats to US national security go well beyond military targets and affect all aspects of society."[65] Until this authority and responsibility bridge between military and commercial industries is closed, cyber vulnerabilities for critical national infrastructure will continue to exist. One needs only to look within the federal government to see these gaps exist; then one can imagine the void between government and commercial entities.[66] By defining domestic policy in legislation—which directs national security interests of cyberspace be placed under the

[63] James Forsyth Jr., "What Great Powers Make It: International Order and the Logic of Cooperation in Cyberspace," *Strategic Studies Quarterly* 7, no.1, (Spring, 2013): 106, http://www.au.af mil/au/ssq/digital/pdf/spring_13/forsyth.pdf.

[64] See Betz and Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-power*: 71.

[65] Department of Defense, "*DOD Strategy for Operating in Cyberspace*," July 2011, 4.

[66] See the US Department of Energy's (DOE) inspector general findings regarding dozens of unaddressed cyber vulnerabilities at key DOE facilities, "including ones dealing with nuclear programs." Although cyber vulnerabilities within the DOE has declined from 56 to 38 since 2011, 22 of the open 38 are brand-new vulnerabilities while 16 remained unresolved from previous inspections. This level of vulnerability seems unacceptable to critical national infrastructure; however, without a concern for accountability, who is managing the oversight for responsibility? For further details see Marcus Weisgerber, "Report: DOD Could Save Billions with New Military Strategy," *DefenseNews*, 15 November 2012, http://www.defensenews.com/article/20121115/DEFREG02/311150001/Report-DoD-Could-Save-Billions-New-Military-Strategy.

full responsibility of one agency—publicizing it, and then enabling authorities to enforce the policy, cyber threats can be mitigated and overall cyber security increased.

Enforcing cyberspace policy is not the same as enforcing rules in the other four domains—land, air, sea, and space. For example, when an unauthorized ship enters sovereign nation's waters, it is detected, action is taken by the responsible agency, and attribution is quickly determined. The same actions can occur in air and space. The same is not necessarily true for cyberspace; at least not today. In America, if a military cyber-force were to offer help to a non-governmental agency, this act would be a violation of the Posse Comitatus Act of 1879; unless authorized by Congress first . Current regulation "restricts the use of military forces in civilian law enforcement within the United States, unless it is within a federal government facility."[67] Given these challenges, a first place to start with enforcement of cyber-security is by evaluating roles and responsibilities of those tasked with protecting cyberspace.

Table 9 below highlights some of the disparate roles that seemingly share lines of operations. If after reviewing the different title responsibilities and the agencies tasked with executing its assigned role, the reader walks away with a clear understanding of who is executing what and under what authority, while understanding a clear break in the lines of responsibility, then the reader is doing better than many professionals operating in the cyber realm. For example, if cyber-attacks are occurring and US corporate secrets are being stolen, who is responsible for recognizing the attack, reporting the attack, stopping the attack if it is in progress, take immediate action to stop the attack, recover the data, and shut down the attackers capability to prevent further attacks?[68] Are all of these options viable? Should they all be executed once an attack is identified?

Responses to the questions above will be as varied as the number of individuals asked to answer. In reality, they should not be. If someone walked into your home and stole a personal piece of property, there are legal rules governing that action, along with responsible agents to act on behalf of the offended. The same goes for corporations. If

[67] Eric Fischer, "Federal Law Relating to Cybersecurity: Discussion of Proposed Revisions," *Congressional Research Service Report for Congress*, 9 November 2012, 20, http://www.fas.org/sgp/crs/natsec/R42114.pdf.

[68] See recent concerns between the US and China regarding the loss of US corporate secrets due to cyber-attacks. Editorial, *The Washington Post*, "US Presses China on Cyber Attacks," 20 March 2013, http://www.washingtonpost.com/world/asia_pacific/us-presses-china-on-cyberattacks/2013/03/20/ef11a3d0-916a-11e2-9173-7f87cda73b49_story html.

one company steals a patent protected idea from another company, there are rules in place to file a claim and potentially recover the losses. Those who conducted the illegal act are then held responsible for restitution and costs associated with legal action. Can cyber-security laws be done the same way? If so, they undoubtedly must occur at a much quicker rate than the examples above.

Table 9

US Cyber Authorities and Current Title Responsibilities

Title	Key Focus	Principle	Role in Cyberspace
Title 6	Homeland Security	Department of Homeland Security	Security of US cyberspace
Title 10	National Defense	Department of Defense	Organize, Train, & Equip US military forces for Offensive & Defensive Cyber Operations (OCO & DCO)
Title 18	Law Enforcement	Department of Justice	Crime prevention, capture, and prosecution of criminals operating in cybercrime
Title 32	US national defense and civil support	State Army & Air National Guard	Domestic consequence management
Title 40	Chief Information Officer	All Federal Departments and Agencies	Establish and enforce standards for acquisition and security of information technologies
Title 50	Military, foreign intelligence, and counterintelligence activities	Commands, Services, and agencies under DOD and agencies under ODNI	The essential authority for Computer Network Exploitation (CNE)

Source: Unpublished Bullet Background Paper by Headquarters, US Air Force Bullet Background Paper, "US Code-Based Authorities Relevant to Cyber Operations"

For cyber-security to work, overlaying the existing principles for national defense in the other four domains may not be the solution. The speed at which cyber-attacks occur, change, re-occur, or stop is what makes cyber-security so much different than any other warfare domain. The time available to conduct inter-agency coordination between domestic and international cyber forces—Title 32: National Guard and Title 18: Law Enforcement versus Title 10: National Defense—will not exist during an initial cyber-attack. To be successful at detecting and mitigating these threats, an agency with full responsibilities for cyber-security may be required. Within such an agency a cyber-force with existing 'Title' responsibilities would eliminate confusion regarding lines of responsibility. It might also consolidate all military, civilian, and corporate entities under one authority for policy standardization and efficient execution. It is important to remember, especially in democratic societies like the US, that this attempt to standardize cyber-security policy and enforcement is intended to focus on national security interests. This effort could expand to private-industry based on the choice of each business to opt-in or opt-out to the stringent requirements set by this new organization; but that is not the recommendation here. It would not be mandated for any industry not deemed critical to national security.

No matter what course of action the US chooses to move down the path for increased cyber-security, any path toward defining acceptable standards, publishing domestic and international policy, and empowering an over-arching cyber-force responsible for US cyber security of national security interests, is a move in the right direction. The US cannot continue down the path of having “no overarching framework legislation in place” for cyber-security.[69] The current path is costing the US an unquantifiable amount of technological and economic loss.[70]

Centers of Gravity and Cyberspace

Lieutenant General Larry James, the Deputy Chief of Staff for Intelligence, Surveillance, and Reconnaissance, Headquarters US Air Force, recently sponsored a study to “determine how the Air Force can better integrate cyber and space target intelligence analysis and materials to create cross-domain target intelligence.”[71] Although the findings of this study are not projected for completion until October 2013, it undoubtedly supports the 2012 Air Force Targeting Roadmap initiative. Managed by the Air Combat Command, the Air Force Targeting Roadmap is intended to “provide fundamental guidance on how to better organize, train, equip, conduct, and manage [Air Force] targeting-related personnel and resources to ensure efficient and effective targeting operations during peacetime, contingency, and war.”[72] Inherent in two of the five focus areas within the roadmap is the concept of centers of gravity. Understanding

[69] Eric Fischer, “Federal Law Relating to Cybersecurity: Discussion of Proposed Revisions,” *Congressional Research Service Report for Congress*, 9 November 2012, http://www fas.org/sgp/crs/natsec/R42114.pdf.

[70] To see estimates of what some US companies, as well as other nations, are spending to counter cyber threats, or repair losses caused by cyber-attacks, see Ponemon Institute, “Second Annual Cost of Cyber Crime Study,” Benchmark Study of US Companies, August 2011, https://www.hpenterprisesecurity.com/collateral/report/2011_Cost_of_Cyber_Crime_Study_August.pdf.

[71] Information provided by Major Chad Manifold, SAASS Class XXII, “Project Air Force Project Description Improving Air Force Target Intelligence,” November 2012.

[72] Roadmap provided by Brigadier General Shwedo, Director of Intelligence, Air Combat Command, “Air Force Targeting Roadmap: Reinvigorating Air Force Targeting,” 30 September 2012.

centers of gravity will not only drive a focused intelligence gathering campaign, it will drive strategic thinking and planning before and during engagements with an adversary. For these reasons, it is critical not only for the Air Force intelligence community to understand centers of gravity, but for all cyber-forces who plan and execute all organize, train, and equip functions to understand them as well; along with those who lead these forces. Additionally, understanding these concepts allows for introspect of friendly vulnerabilities as seen by the adversary.

Published doctrine is a starting point to understand potential centers of gravity. Understanding US military doctrine is important for today's warriors, but so is having an understanding of doctrine and military thinking around the world. A 2007 publication by the Military Science Publishing House in Beijing claims information warfare aims at "seizing control of information" and "is a new form of war."[73] The publication goes on to claim, "Whoever gains information supremacy in war will hold in his hands the initiative of war," and that "information capability has become the most important indicator to evaluate combat capability."[74] Beliefs such as these, combined with tautology like, "The Kosovo War was the first war to involve cyberspace confrontation and that every war since would involve cyberspace confrontation, present the growing importance of cyberspace.[75] Despite the fact that a true cyber-war, in the sense of two air forces or two ground forces battling it out until political objectives are achieved, has not occurred, nations continue to enhance cyber-warfare capabilities. One aspect of improving cyber-warfare readiness for United States forces is to understand centers of gravity concepts in order to either achieve or aid in the achievement of combatant commander requirements. This is especially true when governments around the world consistently identify "US logistics and C4ISR systems as the most important centers of gravity to target in a conflict" in the future.[76]

It is important to define the concept of centers of gravity. First, Clausewitz called centers of gravity, "the hub of all power and movement, on which everything depends."[77]

[73] Xinxi Duikang Lun, *Information Confrontation Theory*, China Publication Library, 2007, Ch 4.
[74] Xinxi Duikang Lun, *Information Confrontation Theory*, China Publication Library, 2007, Ch 4.
[75] Xinxi Duikang Lun, *Information Confrontation Theory*, China Publication Library, 2007, Ch 4.
[76] B.A. Krekel et al., *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage* (CreateSpace Independent Publishing Platform, 2012), 32.
[77] Clausewitz, Howard, and Paret, *On War*: 595.

Second, Joint Publication 5-0 defines centers of gravity as, “a source of power that provides moral or physical strength, freedom of action, or will to act.”[78] Finally, the third publication referenced for centers of gravity is MCDP-1—Warfighting. The short version of the US Marine Corps Doctrine states “centers of gravity are any important sources of strength.”[79] To help determine centers of gravity, MCDP-1 asks three questions: “Which factors are critical to the enemy? Which can the enemy not do without? Which, if eliminated, will bend him most quickly to our will?”[80] From each of these definitions, the common attribute is determining where the center of power comes from. Whether this power provides moral or physical strength, or enables freedom of movement or action are all derivatives of the enabling power.

The human body provides an incredible example for illustrating centers of gravity analysis. Without a heart, the human body would not function as intended. A counter-argument is that today’s technology can keep a human body alive with an alternative power source. Regardless of this argument the center of gravity is still the same; albeit it in a different form. The point is that the brain, which might be confused as a source of power, can provide the will for action, while the physical body provides the capability. The hands and feet provide physical strength and movement, but again, are attributes of ‘the system’ and not the center of gravity of the human body. Without blood flow and oxygen the brain would cease to function and eventually the control center for the body—a system—would cease to operate together coherently. This analogy may lead to questions for the strategist who seeks a true understanding of centers of gravity. Although not an inclusive list, example questions include, how does one differentiate between true centers of gravity and attributes of the system surrounding a center of gravity? To employ resources efficiently and not waste them as Clausewitz warns against, it is critical to focus on true centers of gravity. Another question may be, is there more than one center of gravity in war and can it change? To help answer these questions we turn to Dr. Joe Strange of the USMC War College and Colonel Richard Iron of the UK Army.

[78] Joint Publication 5-0, *Joint Planning,* III-22, http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf.
[79] Marine Corps Document Publication (MCDP) – 1, *Warfighting*, 46, http://community.marines.mil/news/publications/Documents/MCDP%201%20Warfighting.pdf.
[80] Marine Corps Document Publication (MCDP) – 1, *Warfighting,* 46, http://community.marines.mil/news/publications/Documents/MCDP%201%20Warfighting.pdf.

Aside from interpreting Clausewitz's theories on centers of gravity and highlighting misinterpretations between his true meaning and the perceived meaning by practitioners of warfare since the writing of *On War*, Strange draws out two distinct characteristics relevant to understanding centers of gravity. First, the "physical centers of gravity [which] function as active agents;" which he says "endeavor to destroy the enemy's capability and will to resist."[81] In other words, this physical center of gravity may be an army, navy, or air force. Just think about a physical capability. The second characteristic is "moral centers of gravity [which] function as active agents that influence or control physical centers of gravity."[82] Drawing upon Clausewitz's examples, Strange highlights, "the capital" in countries of domestic strife, or "community interests" among alliances, and finally "personalities of the leaders and public opinion" in popular uprisings, as specific moral centers of gravity. In other words, moral characteristics are not easily measured or identified, let alone easily targeted, during warfare. Thus we begin to see the challenges to identifying centers of gravity. If destroying centers of gravity is integral to the rapid conclusion of war, accurately identifying them is an absolute must.

Physical centers of gravity appear definable through effective intelligence resources and analysis of the enemy as a system. If the nation relies heavily upon a military force as its mechanism to mitigate or deter threats, then most likely that force is a center of gravity for that nation. That same force may be a moral center of gravity to the society and political body relying on the force for protection. If defeat were to befall the force, the will of the nation may fall with it—but that is not a guarantee.[83] To help bring clarity in identifying centers of gravity, we lean once again on Dr Joe Strange and Colonel Richard Iron.

Strange and Iron in their second publication on centers of gravity analysis describes a useful model with four inter-related concepts:

[81] Doctor Joe Strange and Colonel Richard Iron (UKA), "Understanding Centers of Gravity and Critical Vulnerabilities: Part 1, 9, http://www.au.af mil/au/awc/awcgate/usmc/cog1.pdf.
[82] Doctor Joe Strange and Colonel Richard Iron (UKA), "Understanding Centers of Gravity and Critical Vulnerabilities: Part 1, 10, http://www.au.af.mil/au/awc/awcgate/usmc/cog1.pdf.
[83] For more examples of what constitute physical and moral centers of gravity, along with questions to ask to help determine what might constitute moral centers of gravity, see Doctor Joe Strange and Colonel Richard Iron (UKA), "Understanding Centers of Gravity and Critical Vulnerabilities: Part 1, 11-5, http://www.au.af mil/au/awc/awcgate/usmc/cog1.pdf.

1. Centers of Gravity (CG) are physical or moral entities that are the primary components of physical or moral strength, power, and resistance
2. Critical Capabilities (CC) are capabilities that can destroy something, seize an objective, or prevent you from achieving a mission
3. Critical Requirements (CR) are conditions, resources, and means that are essential for a center of gravity to achieve its critical capability
4. Critical Vulnerabilities (CV) are those critical requirements vulnerable to neutralization or defeat [and] contribute to a center of gravity failing to achieve its critical capability[84]

Examining this model one concludes that critical capabilities and requirements are inherent to critical vulnerabilities and those critical vulnerabilities are essential targeting objectives to defeat an adversary's center of gravity. With training, strategists and planners can apply this model "to any conflict," in order to determine target objectives.[85] As is often the case, historical analysis concludes true centers of gravity post-hostilities; however, it is this same historical analysis that helps shape better decisions in determining centers of gravity to target in the future. The challenge is figuring out how to use all available intelligence resources to understand the adversary and analyze past experiences to identify what an adversary's physical and moral centers of gravity are before hostilities begin; then remain vigilant to any changes once warfighting begins.

Strange and Iron conclude their model with an overview of centers of gravity and critical vulnerabilities in the 1991 Gulf War Campaign against Iraq. Although the view presented by Strange and Iron appears to be ground centric, their example works well with our Chapter 3 overview of a contemporary airpower theorist, retired Colonel John Warden. The associations are similar in that both models are defined by objectives and focus on centers of gravity. Using Strange and Iron's model, the overall campaign had the following centers of gravity and critical vulnerabilities listed in Table 10.[86]

[84] For full details and specific examples of each concept within the model, see Doctor Joe Strange and Colonel Richard Iron (UKA), "Understanding Centers of Gravity and Critical Vulnerabilities: Part 1, 7-16, http://www.au.af mil/au/awc/awcgate/usmc/cog2.pdf.

[85] Doctor Joe Strange and Colonel Richard Iron (UKA), "Understanding Centers of Gravity and Critical Vulnerabilities: Part 1, 18, http://www.au.af.mil/au/awc/awcgate/usmc/cog2.pdf.

[86] Doctor Joe Strange and Colonel Richard Iron (UKA), "Understanding Centers of Gravity and Critical Vulnerabilities: Part 1, 18-9, http://www.au.af.mil/au/awc/awcgate/usmc/cog2.pdf.

Table 10

1991 Gulf War – Centers of Gravity & Critical Vulnerabilities

	Strategic	Operational	Tactical	Physical	Moral	COG	CV
Saddam Hussein	X				X	X	* Command and Control
Iraqi integrated air defense system (IADS)		X		X		X	US high-tech, electronic, and stealth capabilities
Republican Guard		X		X		X	Dependence on friendly reconnaissance assets and unable to see through smoke and haze
Iraqi Artillery Units			X	X		X	Dependence on IADS and Republican Guard to keep US-Coalition forces at bay

* Command and Control was not listed as a critical vulnerability by Strange and Iron. This was added by the author based on his understanding of the first ring in Warden's Model

(Source: Derived from Doctor Joe Strange and Colonel Richard Iron)

Final thoughts before concluding the centers of gravity analysis is that during course of analysis development, both enemy and friendly centers of gravity should, when possible, be analyzed and considered before engaging in conflict. Also, propositions regarding improvements in defining centers of gravity, or their attributes should not be overlooked. Just as the character of war continues to evolve, so too does the warfighter's understanding. The suggested theory that "future critical factors" influence "critical factor analysis" in later phases of warfare may be one such example.[87] By staying abreast of doctrinal changes, strategic think-tank discussions, and academic research, military commanders will be well suited for tomorrow's war—should it come.

Given today's reality that many warfighting capabilities rely directly, or indirectly—from command-and-control, global positioning, information, surveillance, and reconnaissance, precision munitions, and much more—upon cyberspace, and the fact that military organizations around the world believe that information warfare "is a new form of war," the criticality of conducting full spectrum operations in, through, and from cyberspace is evident in the future success in war.[88] By maintaining an understanding of

[87] For full details regarding critical factor analysis and future critical factors see Jan Rueschhoff and Jonathan Dunne, "Centers of Gravity from the Inside Out", *Joint Forces Quarterly* 60, (1Q, 2011), http://www.ndu.edu/press/jfq-60 html.

[88] Xinxi Duikang Lun, *Information Confrontation Theory*, China Publication Library, 2007, Ch. 4.

the centers of gravity presented by Strange and Iron, and applying the concepts of an enemy as a system presented by Warden in chapter 3, practitioners of cyber-warfare have many lessons to draw upon for success. However, this art-of-war is not for cyber-warriors alone, but for commanders in all domains of warfare to understand and incorporate across weapon system platforms and warfighting domains alike. This will aid not only in the development of the AF cyberpower targeting theory presented in chapter 5, but cyberpower doctrine for US military forces and policy-makers alike.

Additional Artifacts for Further Evaluation

There is a plethora of artifacts beyond the attribution, authority, and centers of gravity discussed that affect cyberpower and those who choose to wield it for war. Three additional areas this author considers for in-depth analysis include escalation, proportionality of cyber-warfare, and the morality of cyber-war. Specifically, have these areas changed the nature of war as some have argued? Or is cyber-war the continued advancement in warfare given new technologies resulting in a character change of war?

From cavalry, to gunpowder, to mechanized infantry, to airpower, each change in technology led to changes in how warfare is conducted. The stirrup is said to be the "third [evolutionary] period" of the use of the horse in battle.[89] The stirrup "replaced human energy with animal power, and immensely increased the warrior's ability to damage his enemy. It made possible mounted shock combat."[90] Gunpowder led to rifles which replaced the long bow and cross-bow. Once rifles were used, experience and continued advancements in technology allowed for increased rifling techniques and better accuracy, along with advancements in the weapons themselves. Ultimately the mass production of rifles allowed infantry to increase the volume of fire thus creating an advantage for those who used it. Next, mechanized infantry sought to replace mounted cavalry and speed the rate of warfare. Finally, the advent of airpower enabled adversaries to occupy the vertical flank of the day. For nations who can afford the technology and employ airpower effectively, airpower enables true control of the battlefield. Airpower,

[89] Lynn White Jr., *Medieval Technology & Social Change*, (Oxford University Press: 1964), 2-27.
[90] Lynn White Jr., *Medieval Technology & Social Change*, (Oxford University Press: 1964), 2.

however, did not eliminate the need for ground forces to hold the battlefield once the enemy had withdrawn or been defeated.

The intent of this very short historical review is to highlight what the author deems are critical technological milestones that directly affected the conduct of warfare. In other words, these changes in technology drove innovative means, employment methods, and doctrinal changes, but none of them led to a change in the nature of war. David Lonsdale captures this point when he claims, "The nature of war is the same as it was in all past and all future ages!"[91] Despite Lonsdale's proclamation, some confusion regarding whether or not the nature of war changes may come from Clausewitz's claim that "war is a chameleon because it changes nature in some degree."[92] However, it is important to understand the rest of Clausewitz writing before claiming that Clausewitz believed the nature of war changes. Clausewitz goes on to say, "War as a whole [is] in relation to the predominant tendencies which are a trinity: primordial violence; probabilities and chance; and subordination of a political instrument."[93] In more simple terms, Clausewitz trinity is best understood as "the people; the general and his army; and the Government."[94] With this understanding, it may be more accurate to restate that when Clausewitz said "war is a chameleon because it changes nature in some degree," he was referring to the character of warfare and used the word "nature" in the sense that with new technology, an evolution in the conduct of war would occur. Without further digression, the intent here is to highlight what can be learned from past changes in warfare while accepting the fact that the nature of war has not, and will not change, and recognizing the character of war has and will continue to change with each new technology.

Specifically, how have the previous changes from the stirrup, to gunpowder, to mechanized infantry, to airpower, changed the potential for escalation and proportionality of warfare and morality in war? Are there patterns to these changes that can shape cyber-warfare doctrine and tactics, techniques, and procedures for tomorrow's military? How do military forces employing cyberpower measure the risk of unintended consequences

[91] Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future*: ix.
[92] Clausewitz, Howard, and Paret, *On War*: 89.
[93] Clausewitz, Howard, and Paret, *On War*: 89.
[94] Clausewitz, Howard, and Paret, *On War*: 89.

when launching a cyber-weapon? Can those forces minimize collateral damage to a target in or through cyberspace like a precision guided munition, or special operations team? How do warriors of tomorrow not become catatonic to the loss of life so far removed from the battlegrounds where blood is spilled? These are difficult questions. If cyberpower can cause catastrophic kinetic damage like some believe, the author included, how primordial is the violence when the enemy has no face but is rather an 'Enter' key away from destruction? Maybe cyber warfare truly enables countries to fight what Trinquier calls "modern war; war that allows the military to kill more and more of the enemy at greater and greater distances, thus reducing the cruel and brutal physical contact with the enemy."[95]

Summary

Attribution, authorities, and centers of gravity are but a few of the critical aspects to wielding cyberpower effectively. Although 100 percent certainty regarding attribution is desired, it may not always be attainable. If the US is going to curb the growing trend of cyber-attacks against areas of interest regarding its national security, a change in strategy is required. This change is obviously not a one-shoe fits all strategy; there will be trial and error as it will not be right the first time. By publicizing US intentions regarding offensive and active-defense cyber-operations, the US will begin to put enforcement mechanisms behind the rhetoric of previous years in regards to cyber-security. When adversaries can expect a response to threats they initiated, the cost of any cyber-attack goes up theoretically.[96] Now the adversary must determine the benefit gained from their action; potentially more so than has been done in the past.

The level of response, and authority to conduct such a response, may change with each cyber-event. The US must remove the paradigm chains caused by operating in various warfighting domains. There may be some laws and rules of engagement that can be spread across the spectrum of conflict, but others may not easily support cyberspace operations. Those gaps must be exploited before war begins and cyber-operations are

[95] S.N. Kalyvas, *The Logic of Violence in Civil War* (Cambridge University Press, 2006), 53-54.

[96] Deterrence theory is once again referenced as a basis for understanding adversary actions and reactions based on unacceptable threats and credibility of response by a nation or actor. T.C. Schelling, *Arms and influence* (YALE University Press, 2008).

employed. If not, delays to operations will surely occur which will put the US behind in the observe-orient-decide-act (OODA) loop decision cycle, thus potentially losing valuable time and effects against the adversary.

Finally, understanding centers of gravity, both those of the US and of potential adversaries, will shape the battlefield. It can also drive pre-war efforts to organize, train, and equip forces so when warfare begins, forces are not then beginning to understand how to use cyberpower effectively to influence, disrupt, degrade, destroy, or control an adversaries capabilities through cyberspace operations. Developing critical capability, critical requirement, and critical vulnerability descriptions can help shape early operations and identification of true centers of gravity. Without them, delays to all five warfighting domains may occur.

These three artifacts of cyber operations are but a small piece to the chaoplexic environment known as cyberspace.[97] The proverbial tip of the iceberg is what these three areas represent. What concerns warfighters, and potentially policy-makers who guide warfighting actions, is the 80 percent of the iceberg remaining below the surface that we have not begun to think about critically, nor truly understand the complexities they bring to this technologically globalized world in which we live. However, for the Air Force, that is exactly what the remainder of this thesis attempts to address. What should the US Air Force target with cyberpower? Can Air Force cyberpower have strategic impact? Does an Air Force cyberpower targeting theory help the service to organize, train, and equip cyber-forces for tomorrow's wars?

[97] Chaoplexity is defined as the increasing application of computers to the study of scientific problems, the rediscovery of non-linear mathematics, and an extension of the cybernetic analysis of systems to questions of self-production and self-organization constituted new scientific approaches which crystallized in the theories of chaos and complexity. For more specifics, see: Bousquet, *The Scientific Way of Warfare: Order and Chaos on the Battle Fields of Modernity*: 34.

Chapter 5

Hypothesizing a Cyberpower Targeting Theory

> *To say that strategic theory for cyberpower currently is still in its infancy would be a gross understatement.*
>
> Colin Gray

> *Any Air Force which does not keep its doctrines ahead of its equipment, and its vision far into the future, can only delude the nation into a false sense of security.*
>
> General Henry H. Arnold

Introduction

The goal of this chapter is to focus all previous chapters toward the objective of developing a strategic cyberpower targeting theory. To do this, we first must have a common understanding of warfighting. As we strive to develop a theory, the words of Clausewitz are immortal, "Theory should be study, not doctrine."[1] The intent is not to create doctrine or advocate for only one way in which cyberpower can be effective, as early airpower advocates did with strategic bombing.

As the chapter develops, Clausewitz is relied upon for the traditional reference and understanding of war and warfare, along with other definitions found in US doctrine and established by contemporary authors. Next a foundation for theory development is provided by Dr. Winton's "An Imperfect Jewel" article.[2] An explanation of what Dr. Winton contrived as requirements for a theory came from his review of Clausewitz. These requirements are provided, along with an additional requirement deemed necessary by the author to round out theory development. Finally, a cyberpower targeting theory is offered for USAF cyber efforts, although the author believes its value transcends a specific military service and has application at the DOD and national level.

Since the initial question of this treatise is based on the inquiry of what airpower could offer in developing a cyberpower targeting theory, the author argues the evolution of airpower strategies forms a foundation for this theory. Cyberpower is in its infancy

[1] Clausewitz, Howard, and Paret, *On War*: 141.

[2] See the full article of Dr. Harold Winton's, "An Imperfect Jewel: Military Theory and the Military Profession," *The Journal of Strategic Studies* 34, no. 6, 853-877.

and has had one central focus on defensive cyber operations—much like strategic bombing had one central focus by early airpower theorists and studies at the ACTS. The challenge to this limited thinking, the author argues, is it narrows the focus of cyberpower capabilities to a realm that minimizes full spectrum cyber capabilities in support of Combatant Commander Requirements during war.

Clausewitz stated the outcomes of battle are recognized by three distinct signs: psychological; wasting away one's own troops faster than the enemy; and ground lost.[3] Unless cyber-operations are used offensively in all phases of military operations, full capabilities go unrecognized. The defensive use of cyber as the primary role of US military, specifically Air Force cyber forces, forgoes the dogma that "all war presupposes human weakness, and seeks to exploit it."[4] To exploit weakness, offensive action is required.

Today's US military cyber efforts appear very similar to the early 1920's of the ACTS. ACTS taught airpower projection through unescorted strategic bombing of industrial capabilities known as the Industrial Web Theory. The ACTS team, through continued study of warfare and theoretical application of airpower, eventually realized that unescorted bombers required fighter escorts to prevent exponential bomber force loses. The use of combined arms was not new to warfighting as historical examples of ground and naval warfare abound. In fact, the USMC has built the Marine air-ground task force around the concept of task organized ground, aviation, combat service support, and command elements. This structure offers commanders a single combined arms force for flexible response.[5] The Army Air Corps learned valuable lessons with their combined bomber offensives in World War II and thus stuck with the strategy of a combined bomber offensive through the Korean and Vietnam Wars. The similarity to military cyberpower efforts today are generally focused on defensive operations and focus on supporting other domain operations vice developing independent offensive and exploitation action. Cyberpower theories today should evolve before the next war and

[3] Clausewitz, Howard, and Paret, *On War*: 250.

[4] Clausewitz, Howard, and Paret, *On War*: 256.

[5] For an understanding of the combined arms concept see United States Marine Corps, MCDP-1, *Warfighting*, 20 June 1997, 55.

consider how full spectrum cyber capabilities can be used by viewing the enemy as a system.

Colonel Warden's concept of the "Enemy as a System" directly shapes the concepts espoused in the following theory.[6] It also provides a historical warfighting theory for airpower that directly correlates to cyberpower; although cyberpower potentially has a greater holistic effect than airpower alone due to the integration of cyberspace into every aspect of the five warfighting domains—land, sea, air, space, and cyber. By focusing on the enemy as a system, cyberpower can target centers of gravity either independently or integrated with engagements within other warfare domains to bring an expedient end to an adversary's *capabilities and will* to wage war.

It is important to note that during the development of a cyberpower targeting theory, this author forgoes the argument of whether technology or doctrine should come first in order to build cyberpower capable of delivering effects. Colin Gray highlights the challenges incurred during airpower theory development while concluding that it is irrelevant as to whether doctrine or technology comes first, but rather "the focus must first be expanded to encompass the whole of a conflict."[7] Just as Colin Gray believes airpower theory should be "conceived, designed, and executed in the context of war and warfare as a whole," so this author believes a cyberpower targeting theory should embrace the same context.[8]

Understanding Warfighting: A Foundation to Cyber-warfare

Unfortunately a military definition of warfighting is not offered in Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*.[9] To understand how a military capability is used in warfare, it is undoubtedly instrumental for the warfighter to understand the concept of warfighting in relation to the conduct of war. For this reason we turn to US Marine Corps doctrine.

[6] Olsen, *John Warden and the Renaissance of American Air Power*: 108.
[7] Colin Gray, "The Airpower Advantage in Future Warfare: The Need for Strategy," Air Force Doctrine and Development Education Center, Research paper 2007-2 (December 2007), 8.
[8] Colin Gray, "The Airpower Advantage in Future Warfare: The Need for Strategy," Air Force Doctrine and Development Education Center, Research paper 2007-2 (December 2007), 8.
[9] Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 317.

Warfighting, as described in MCDP 1, requires an understanding of the nature and theory of war and must be the guiding force behind preparation for war.[10] This should be inherent to any warfighter who understands their role and responsibility in protecting national security, while upholding the subservient role of a military as just one *means* to achieve political objectives. Despite whether the military is the first or last instrument of power chosen by political leaders, militaries must be prepared to execute in all warfighting domains when called upon.

To execute warfare effectively, military commanders must understand the art-of-the-feasible and science-of-the-probable in each warfare domain called to action. Knowing what is technically capable based upon current technologies avoids over-promising on capabilities, as some believe was the case with early airpower efforts and the strategic bombing advocated throughout World War II and beyond.[11] It also helps address the perpetual concern Colin Gray highlights as inherent to literally every dimension of US military power. He states "US military power is fraught with conceptual uncertainty."[12] Relative to cyber, Gray goes on to argue "cyberwar [is] bereft of strategic theory tailored for the realms of behavior."[13]

The author posits a different perspective than Gray in that US military power is not fraught with conceptual uncertainty relative to the capabilities inherent to militaries, but rather the unknown use and effectiveness of those capabilities in the next engagement. Compound that unknown with the development of new and continually evolving technology and the proliferation of uncertainty becomes evident. Clausewitz succinctly identifies these unknown challenges as "uncertainty of information," which is further simplified as the fog and friction of war.[14]

[10] United States Marine Corps, MCDP-1, *Warfighting*, 20 June 1997, 71.

[11] See how American air force leaders believed they could overcome the obstacles British air forces encountered during the combined bomber offensive when Americans entered the war in 1942. Initially Americans were against using aerial weapons to bomb civilians and civilian targets, however after heavy losses in August 1943. A flawed doctrine and belief was that bombers could defend themselves in massed formations. Further details are in Y. Tanaka and M.B. Young, *Bombing Civilians: A Twentieth-century History* (NEW Press, 2010), 36-37.

[12] Colin Gray, "The Airpower Advantage in Future Warfare: The Need for Strategy," Air Force Doctrine and Development Education Center, Research paper 2007-2 (December 2007), vii.

[13] Colin Gray, "The Airpower Advantage in Future Warfare: The Need for Strategy," Air Force Doctrine and Development Education Center, Research paper 2007-2 (December 2007), vii.

[14] Clausewitz, Howard, and Paret, *On War*: 138.

In the words of David Lonsdale, understanding war relates to how actors prepare for hostilities.[15] "What one perceives as the nature of warfare greatly influences the development of doctrine, force composition, and training."[16] Applying this to the cyber domain, current preparation and employment of cyberpower is on-going in existing military campaigns. Given this fact, it is presumable that cyberpower can support traditional conventional force application methods in each of the other domains. But does cyberpower stop there? Are we currently employing cyberpower as the forward air controller observed ground troop movements for the Army back in the early 1900's? This author believes cyberpower offers much more than being relegated to support roles only and that cyberpower can and should be prepared to act independently; however, it should not be expected to conclude a war on its own. Although, in certain cases, depending on the effects cyberpower can achieve, it is not unforeseeable that cyberpower could conclude a war with the right conditions; depending on the political objectives.

A challenge to military cyberspace operations is the fact that cyberspace is not owned solely by military forces. This concept is different than all other warfighting domains in that bomber aircraft or a naval ships operated by military forces do not require collaboration with civilian agencies to be employed. Military forces must collaborate with civilian owned, managed, and operated cyberspace in order to achieve effects. This interaction blurs the lines of where military actions begin and end compared to those of civilian organizations and their personnel. It also leads intuitively to examining how adversary warfighting capabilities are supported by cyber-operations to determine where, when, and how friendly forces can affect those capabilities during war; without regard to an adversary's military or civilian lines of coordination. Understandably some will view this as a Douhetian style of "bombing cities and factories instead of military forces," but that is not the intent.[17] The intent is to focus strategists thinking away from just the military forces of an adversary and toward understanding the enemy as a system to aid cyberpower target development and planning effects.

[15] Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future*: 22.

[16] Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future*: 22.

[17] Douhet captured the idea of crushing the material and moral resistance of the enemy without regard to military or civilian losses in the first of his eleven principles of air power. Douhet et al., *The Command of the Air*: 128-29.

Cyberpower can be decisive in an engagement by itself, or it can function in a supporting or supported role relative to other warfighting domains. This will require coordination, as Robert Pape suggests, in that militaries must forgo the “loss of institutional autonomy” to maximize military effectiveness.[18] The interoperability of cyberpower with other military—and civilian—instruments of power is relatively unknown and untested, but that should not inhibit thinking about how to improve its capabilities. Unlike Pape’s argument that threats to civilians by airpower are wasteful and immoral, this author argues military cyberpower is wedded to countless civilian cyberspace operations and therefore requires civilian inclusion when determining threats and threat response actions—or “sticks and carrots”.[19]

Anyone who claims a single warfighting domain can function independently and win a war should cause others to question the validity of their assertion. History of past wars clearly shows this is not the case. However, each domain must be prepared to operate independently, as well as collectively, when called upon. Since most wars of the future will probably be limited in nature, the military desire to employ full military capabilities from the onset of war through its conclusion is unlikely; no matter how desirable by a commander. For this reason, the propensity of escalation from low-intensity—limited war—toward high-intensity—total war—appears likely when compared to the days of planned engagements on the battlefield where opponents met and a clash ensued until a decision was reached.[20]

If escalation is how future warfighting will evolve versus non-war one minute and total war the next, then militaries must ask themselves how they are preparing for warfare in cyberspace. How are US military cyber-forces preparing to respond to calls for

[18] Pape, *Bombing to Win: Air Power and Coercion in War*: 331.

[19] Pape, *Bombing to Win: Air Power and Coercion in War*: 331.

[20] The author’s use of absolute or total versus limited war is based on an understanding of Clausewitz in that total war places “no logical limit to the application of force.” In other words, opposing forces will use “total means at his disposal” to overcome an enemy. The author calls this theoretical warfare and suggests this is the warfare military commanders prefer as there are no limits on capabilities and actions in warfare which would theoretically aid in rapid capitulation by an adversary. However, as Clausewitz develops his theory of war, he reminds readers of the difference in desired war and reality; or what he calls war in practice, not what its ideal nature ought to be. Future wars described by Clausewitz “will be severely restricted.” Limited aims of warfare will dictate limited offensive and defensive war. These limitations are the product of the nature of political aim, the scale of demands put forward by both sides, and the total political situation of one’s own side. Wars conducted by the US since World War II where unconditional surrender was required appear to favor limited verse absolute warfare described. Clausewitz, Howard, and Paret, *On War*: 593-602.

national-level cyberpower application, specifically when the US has not defined what constitutes cyber war or cyber warfare? More directly, how is the USAF preparing for the strategic use of cyberpower? Do cyber-warriors understand the nature and theory of war to guide preparations which MCDP 1 requires? Will a cyberpower targeting theory aid the development of doctrine, force composition, and training as Lonsdale suggests?

Determining whether cyber-warriors understand the nature and theory of war is beyond the scope of this work. Since our focus is on the AF, the scope is limited to the chain-of-command for AF cyber-operations. It is safe to presume commanders of USSTRATCOM, USCYBERCOM, and Twenty-Fourth Air Force understand warfighting concepts. What may be missing is the national institution support required to prepare their forces for cyber warfare. Doctrine is in its infancy, organizational roles and responsibilities are still being fleshed out, and combat experience in cyber warfare is minimal.

It is important to note that doctrine supports operations; it does not dictate them or control them by establishing limiting parameters. MCDP 1 states, "Doctrine must continue to evolve based on growing experience, advancement in theory, and the changing face of war itself."[21] Given the fact that cyber warfare has not occurred overtly, mainly from a perspective that the US has not clearly defined what constitutes cyber war, the USAF has minimal open-source experiences for developing cyber doctrine. Waiting for doctrine to drive military and domestic security of the cyber domain as General Arnold suggests in the opening quote is not an option. Actions are required to protect and defend cyberspace today if the US intends to maintain superiority in all warfighting domains while protecting the nation's most vital security interests. The following principles and proposed theory are intended to provoke thought and action about future US Air Force warfighting in the cyberspace domain; as well as cyberpower projection in all warfighting domains.

Recalling the Principles of War and Applying them to Cyber

The application of cyberpower must be done with consideration of long-standing principles of war regarding force application. Just as the application of military power is

[21] United States Marine Corps, MCDP-1, *Warfighting*, 20 June 1997, 2-3.

projected in the other four domains—land, air, sea, and space—military power can be projected in cyberspace. Reviewing principles of war enables the reader to digest the standing principles and invites critical thinking regarding a proposed cyberpower targeting theory.

As previously mentioned, AFDD – 1 describes the following principles of war for airpower: unity of command, objective, offensive, mass, maneuver, and economy of force, security, surprise, simplicity, unity of effort, restraint, perseverance, and legitimacy.[22] Although these principles are intended to "serve as valuable guides to evaluate potential courses of action" and not a "checklist to guarantee victory;" with this in mind, recent wars have caused the Air Force to develop four additional principles—unity of effort, restraint, perseverance, and legitimacy.[23] The point of highlighting this is, as cyber-warfare evolves, it is incumbent on the practitioners and strategists alike to espouse new principles when required.

The challenge for cyberpower today is, as it was with airpower when initially evaluated for military use, to overcome initial barriers to efficacy in order to achieve warfare objectives in support of political *ends*. Forgoing these challenges, the author focuses on the traditional principles of war and relies upon the works of Dr. Kainikara to briefly explain each one.

Sanu Kainikara of Australia provides an excellent synopsis of standing principles of war derived from the study of Sun Tzu and Clausewitz alike. As Dr. Kainikara suggests, principles of war are the primary guiding elements in the conduct of conflict enshrined in a nation's doctrine; doctrine which normally only changes when radical shifts in national security priorities occur.[24] Without dissecting how the principles of war guide the conduct of conflict in cyber-war, mostly due to a lack of real-world experience, it is appropriate to highlight that principles of cyber-warfare are being developed by some as we will see below. First, Table-11 is a consolidated matrix of standing principles of

[22] Air Force Doctrine Document (AFDD) - 1, *Air Force Basic Doctrine, Organization, and Command*, 14 October 2011.
[23] Air Force Doctrine Document (AFDD) - 1, *Air Force Basic Doctrine, Organization, and Command*, 14 October 2011.
[24] S. Kainikara and RAAF Air Power Development Centre, *Principles of War and Air Power* (Air Power Development Centre, 2011), 6.

war derived from Dr. Kainikara's work by the author.[25] Sticking with the context of airpower as this study's basis, each principle of war has a role in projection of airpower.

Table – 11

Principles of War

Principle of War	**Principle Defined**	**Espoused by Theorist**
Objective	The single path to success in aerial warfare is unwavering adherence to the Principle of Objective. The adaptability of air forces to many missions and the ease with which they may be diverted encourage vacillation and defeat.	General Air Force Principles' Lecture, Air Corps Tactical School, 1934-35
Mass	The principles of war could, for brevity, be condensed into a single word; concentration.	B.H. Liddell Hart, 1930s
Offensive	Air forces characteristically take the offensive. Even in defense, they defeat an invading enemy by attack.	AU Manual 1, USAF Basic Doctrine, 1951
Security	Always presume that the enemy has dangerous designs and always be forehanded with the remedy.	Fredrick the Great, 1740-1786
Surprise	I believe that, more or less, all of the Allied operations [in the Southwest Pacific] depended on deception by landing in places where we thought a landing and the building of airfields impossible.	Lt Col Masaru Shinohara, Japanese Eighth Area Army, 1942-1967
Manoeuvre	An air force commander must exploit the extreme flexibility, the high tactical mobility, and the supreme offensive quality inherent in air forces, to mystify and mislead his enemy, and to threaten his various vital centers…	J.C. Slessor, 1943-1952
Economy of Force	To me an unnecessary action, or shot, or casualty, was not only waste but sin.	T.E. Lawrence, 1914-1935
Simplicity	Avoiding unnecessary complications in the planning, organizing, and conducting of military operations.	S. Kainikara, 2011
Unity of Command	Subscribes to the airpower tenet of 'centralized control and decentralized execution.' This is also evident in the single component commander theory for like forces within an area of responsibility.	S. Kainikara, 2011 and author's interpretation of the Joint Forces Air Component Commander role

Source: Sanu Kainikara, *Principles of War and Airpower*.

Some principles of cyberspace operations are beginning to circulate within the cyber community. Major General Williams developed ten propositions, Table 12 below, regarding cyberspace operations while serving as the PACOM/J6 in Hawaii.[26] His and other principles regarding cyberpower are critical and required; however, it is relevant to understand the context of each. General Williams' is focused on what he calls the

[25] Kainikara and Centre, *Principles of War and Air Power*: 6.

[26] See the propositions General Williams proposes regarding command and control of cyber-force operations by the combatant commander, just as all other warfare domains are currently controlled. He is also an advocate of creating a Joint Forces Cyber Component Commander so the combatant commander has one commander responsible for cyber operations within the combat area of responsibility. See Brigadier General Brett Williams, "Ten Propositions Regarding Cyberspace Operations," *Joint Forces Quarterly* 61, (2Q, 2011).

operational level of warfighting as he espouses control of cyber-forces and operations during war by the combatant commander. The author’s concern is that cyberspace is not confined to a region, despite General Williams’ push to construct the global information grid accordingly, and therefore giving control of cyberspace to a JFC might have unintended consequences to a JFC in a different region. General Williams’s perspective is dependent on the context of the combatant commander at that time and does warrant analysis in order to enhance JFC operational cyberspace capabilities.

Table – 12

Ten Propositions Regarding Cyberspace Operations

Propositions	Author's questions to provoke thought
Cyberspace is a warfighting domain. At the operational level of war, cyberspace operations are most similar to those in land, maritime, and air.	Does cyberspace afford capabilities to multiple JFCs operating in diverse regions? A soldier, naval vessel or an aircraft can only be in one location at a time; cyberspace in one theater can support operations in multiple theaters simultaneously.
The JFC must have C2 of cyberspace, just as he does of the terrestrial domains.	Would a national-level cyber tasking order allow the JFC a medium for executing cyber-targeting objectives? Will a higher-level tasking process afford limited assets (i.e. cyber force operators) to conduct more missions on a broader scope?
C2 of cyberspace is the key enabler for exercising operational command and control.	Is C2 at a higher echelon than JFC make sense so situational awareness across the entire global information grid is understood before a regional JFC executes a cyberspace operation that might affect other regions/operations?
Defense is the main effort in cyber at the operational level of war.	Is defense the main effort for cyber during war, or does the main effort become offense? If offense, should that be the main effort during peacetime as well so OT&E is geared toward wartime objectives accordingly?
Cyber is the only manmade domain. We built it; we can change it. Creating a cyber JOA is the first requirement.	Does this move cyberspace back to days of different operating standards for different forces across the COCOMs?
Cyberspace operations must be fully integrated with missions in the physical domains.	Are barriers to this integration the current security practices, exercise limitations, and
The JFC must see and understand cyberspace to defend it--and he cannot defend it all.	Will automated sensors with passive and active defense systems enhance JFC confidence? Can these be managed from a national level with a local detachment providing instant data to the JFC meet this intent?
Networks are critical and will always be vulnerable--disconnecting is not an option. We must fight through the attack.	When comparing cyber to the traditional domains (land, sea, and air), are there times where forces retrograde or retreat? Should this remain an option for cyberspace operations as well?
Our understanding of nonkinetic effects in cyberspace is immature.	Can virtual ranges, increased real-time cyber operations in recurring exercises, and use in real-world operations grow this understanding? Can the cyber community reduce security constraints within the military community in order to increase lines of communication and understanding between cyberspace capabilities and those of other warfighting domains?
Understanding operational impact is the critical measure of cyberspace engagements.	Does this impact include the readiness of cyber forces through military OT&E actions as well? Is there value in conducting "days without cyber" to test the operational environment during peacetime to better understand potential impacts during combat?

Source: Brigadier General Brett Williams, “Ten Propositions Regarding Cyberspace Operations,” *Joint Forces Quarterly* 61, (2Q, 2011).

Cyberspace as a Warfighting Domain

With a common understanding of warfighting and the principles of war, another artifact to resolve before defining a cyberpower targeting theory surrounds cyberspace as a warfighting domain. The emergence of cyberspace as a warfighting domain is not readily accepted by all and is driven by academics such as Martin Libicki and his challenge to determine military cyberpower. In *Military Cyberpower*, Libicki concludes that the “null hypothesis”—that cyberpower does not matter—remains to be disproved.[27] This author rejects the argument and finds the debate academic in nature and futile in moving military cyberpower forward. The fact is, testing to determine if cyberpower matters or not is irrelevant. It is important! The question is what impacts can cyberpower wielded by an adversary have on US vital interests and how best should US military forces be postured to meet security and political objectives alike? The focus of Libicki’s argument should be on evaluating vulnerabilities of adversaries to cyberspace operations, while identifying friendly critical capabilities and vulnerabilities that must be protected in war given the mass migration of operational reliance on cyberspace.

Cyberspace operations pervade every conventional warfighting domain. Cyberspace not only enhances current operations, new technologies push greater inter-connectedness more each day. This domain does not only affect military operations; it also impacts the very sole of the US’s capitalistic society. From banking, logistics, navigation, air traffic control, electric grids, and much more, the cyber domain is embedded in diverse operations enabling society to function more efficiently each day. Major General Vautrinot, the Twenty-Fourth Air Force Commander, pithily encapsulates the cyber domain as “an environment of intellect, integration, and, for good as well as ill, complex interdependency.”[28]

The US cannot ignore cyberspace as a warfighting domain. To develop this new warfighting domain, it must employ lessons learned throughout history while not being blinded by cognitive dissonance. The nation’s security requires military forces to recognize the new opportunities cyberspace affords protectors of freedom. Creating a

[27] Martin Libicki, “Military Cyberpower,” in Kramer, Starr, and Wentz, *Cyberpower and National Security*: 47.

[28] Major General Suzanne Vautrinot, “Sharing the Cyber Journey,” *Strategic Studies Quarterly* 6, no. 3 (Fall 2012): 72.

cyberpower targeting theory requires an understanding of cyberspace and what is now being called the cyber domain. Accepting or rejecting cyberspace as a domain will either coalesce or divide thinking by strategists and tacticians. Coalescing is what the US must do as it prepares for future war.

Stuart Starr, in "Convergence of Sea Power and Cyberpower," suggest there are 28 candidate definitions of the term cyberspace—but in reality, it only requires one.[29] Forgoing the massive comparison, this treatise employs the National Defense University definition by Starr.[30] Cyberspace is an operational domain whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interconnected and inter-netted information systems and their associated infrastructure.[31] There is one element this author adds to this definition—the human element. Therefore, cyberspace also includes all human elements that create, interact, disseminate, and negate information or the system itself in, through, or from cyberspace. Since cyberspace is a man-made domain, the human element is critical to an inclusive definition.[32]

Cyberspace is a domain equal to air, land, sea, and space. According to Webster's Dictionary a domain is "A territory over which dominion is exercised."[33] Accepting the understanding provided of what constitutes cyberspace, the author posits dominion within cyberspace is probable and already evident. Stuxnet—the cyber-attack on Iranian centrifuges—would not be possible without operations in the cyberspace domain.[34]

[29] An alternative definition, although the author does not believe it is a clear definition, Derek Reveron says cyberspace is considered a fifth dimension where people can exist through alternate persona in virtual reality. See Reveron, *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*: 5.

[30] Stuart Starr, "Toward a Preliminary Theory of Cyberpower," Kramer, Starr, and Wentz, *Cyberpower and National Security*: 47.

[31] Stuart Starr, "Toward a Preliminary Theory of Cyberpower," Kramer, Starr, and Wentz, *Cyberpower and National Security*: 47-48.

[32] See principle five of Major General Williams' ten principles for details regarding the man-made domain and how it can be influenced by man. Brett Williams, "Ten Propositions Regarding Cyberspace Operations," *Joint Forces Quarterly* 61, (2Q 2011): 14.

[33] Webster's Student Dictionary (Trident International Press, 1999), 211.

[34] For information on Stuxnet and its effects, see J. Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare* (Penguin Press, 2011), 102., and Reveron, *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*, 11.

Militaries desire the ability to dominate in cyberspace despite the "Wild West" syndrome.[35] Benefits of operating in cyberspace are theorized, but in reality given the limited battleground in which cyberpower has been wielded, many benefits are speculative at best. Stuart Starr acknowledges some of these benefits when he says that accepting cyberspace as a distinct domain will lead to significant implications toward equipping cyber-forces and developing a culture for cyber activities.[36] This sounds eerily familiar to early airpower supporters who advocated a separate service before 1947. In fact, we are again talking about a new character of military power; one that that can have devastating effects in war just as air, land, and sea power. To be effective, strategists must think about employing a weapon system while striving to understand its effects on the adversary and on meeting political objectives. Theory is a tool to encourage this thinking. One up front challenge to creating cyber theories of any kind is the limited experience which leads to familiarity with the subject of *theory* espoused by Clausewitz.[37] However, that cannot be justification for not trying to develop something useful.

Basis of Theory Development: Wintonian Style

This treatise suggests a cyberpower targeting theory for military cyberpower application in war. It is scoped to the perspective of Air Force cyberpower; although the author hypothesizes the propositions are applicable to DOD and national level cyberwar objectives. Development of a military theory is achieved by employing the Wintonian model which claims that theory—defines, categorizes, explains, connects, and anticipates—as found in Dr. Harold Winton's entitled "An Imperfect Jewel."[38] *Defining* cyber-targeting is the first step and is accomplished by relating definitions throughout the thesis to their importance in cyber-targeting. At the same time, an association of cyber-targeting's importance to warfighting is applicable. The cyberpower targeting theory continues to evolve by *categorizing, explaining, connecting, and anticipating* the use of

[35] Gregory Rattray, "An Environmental Approach to Understanding Cyberpower," in Kramer, Starr, and Wentz, *Cyberpower and National Security*: 274.

[36] Stuart Starr, "Toward a Preliminary Theory of Cyberpower," Kramer, Starr, and Wentz, *Cyberpower and National Security*: 48.

[37] Clausewitz, Howard, and Paret, *On War*: 141.

[38] See the full article of Dr. Harold Winton's, "An Imperfect Jewel: Military Theory and the Military Profession," *The Journal of Strategic Studies* 36, no.6, (19 December 2011): 853-877.

cyberpower as a military instrument of power by focusing cyber-targeting efforts on suggested centers of gravity while using the concept of Colonel Warden's enemy as a system.

The author then injects a final aspect of theory development by adding a *testing* phase to the cyber-theory. This additional step is beyond Dr. Winton's theory model, but one critical to determining a theory's worth. Since the intent of war is to compel an enemy to do one's *will*, and accepting military operations are subservient to political objectives as Clausewitz suggests, the strategist must understand the limits of force and know when political objectives are beyond the reach of military action.[39] Without testing a theory it becomes subjective as to the true worth of any hypothetical theory, and waiting to test it in warfare is undesirable; although warfare provides the most validity compared to preconditioned exercises and testing.

Clausewitz suggests, "theory should be study and not doctrine;" however, if the USAF does not think about cyber doctrine and operational tactics, techniques, and procedures now, then it may be in the same situation airpower forces were in before World War I.[40] Because the US did not have adequate knowledge of military aviation, "the military had to improvise and depend on allies for advanced training of the Air Service."[41] If the USAF develops a cyberpower targeting theory and tests it both in real-world and exercised scenarios, then applicable doctrine with supporting operations such as organize, train, and equip functions can be established. Developing a basic foundation for cyberpower in warfare will enhance coordination with other military services, civilian agencies, commercial industries, and allies. These foundations can expand as additional experiences are gained.

Developing a Cyberpower Targeting Theory

It is important to remember the sage advice of Dr. Winton before developing a theory by remembering that "no theory can fully replicate reality…and military theory

[39] "The political object is the goal, war is the means of reaching it, and means can never be considered in isolation from their purpose." Clausewitz, Howard, and Paret, *On War*: 87.
[40] Clausewitz, Howard, and Paret, *On War*: 75-87.
[41] Finney and History, *History of the Air Corps Tactical School, 1920-1940*, 3.

practically always lags behind the explanatory curve of contemporary developments."[42] Dr. Winton lays out a few key attributes to consider when developing a theory. During the first task one must *define* the field of study under investigation. A relevant example Dr. Winton used was Clausewitz definitions of war.[43] The difference with cyber is unlike Clausewitz who had both history and experience in warfare, there is no attributed experience of cyber-war. For this purpose, we first discuss defining cyberspace, cyber-war, cyber-attack, and then develop cyber-targets to help shape a theory.

The second task is to *categorize*. Using the premise established by Clausewitz that wars can be offensive and defensive is applicable to cyberpower targeting and will be used to develop the theory here. Exploitation will also be added as a third category in which cyber operations can and are being conducted by various nations and individual actors.

Third, Dr. Winton claims "*explanation* is the soul of theory," and the author agrees. By developing a cyberpower targeting theory it is the author's desire that open dialog will occur regarding military expectation and use of cyberpower. It is also an aspiration that by defining specific roles of cyberpower, a derivative product will be development of US policy regarding cyber-attacks, thus creating domestic and international standards of behavior in cyberspace.

The fourth objective is to *connect* cyber-operations to other military domains in order to integrate the newest warfighting domain and its capabilities into established concepts of operation. A bi-product of this attempt to connect military cyber-operations to other warfighting capabilities will potentially highlight gaps between civilian and military roles and responsibilities regarding cyberspace operations relative to cyber vulnerabilities of critical national infrastructure; thus pressing the need for an over-arching US organization to manage cyberspace—something along the lines of a Department of Cyber with USCYBERCOM as the military agency supporting this new organization; much like USNORTHCOM support the Department of Homeland Security.

[42] Winton, "An Imperfect Jewel," *The Journal of Strategic Studies,* 856.

[43] Clausewitz defined war as "an act of force, and there is no logical limit to the application of that force." This definition succinctly defines war for the perspective of this treatise. Clausewitz, Howard, and Paret, *On War*: 77.

A fifth aspect of theory development is to *anticipate*. "Anticipation can be almost as useful as prediction," says Dr. Winton, as he argues action and reaction in the human arena are less definitive.[44] Given the undefined parameters of what constitutes cyber-attacks, and the lack of cyber-war up to this point in history, any cyberpower targeting theory is going to fall definitely into the realm of anticipation. The author's intent is to anticipate how defining cyber-attack, and targets that the US values as critical to national security, might dissuade further attacks on those areas of interest by publicly acknowledging an intended US response to such threats.

The sixth and final factor in this theory, one added by the author, is *testing*. Although there has not been a cyber-war, there have been conflicts in which cyber-attacks were possible and did in-fact occur. In conflicts where cyberpower was not used or not known to the public, the question arises as to why not? Are cyber-attacks limited by the lack of policy and authority given to military commander's to use in the arsenal of weapons within the military instrument of power? The author's argument here is, cyberpower is just that, another arrow in the quiver. Although it is a new capability, it is not a nuclear weapon; therefore, should we be guarding its capabilities like they are nuclear weapons? Given the porous nature of cyberspace, would US interests be better served through demonstration to assist in establishing credibility upon which to build deterrence? A review of the Stuxnet attack will be used to demonstrate the author's intent.

Define

Being the target of a cyber-attack seems to be daily news. It has been somewhat obscure for the past decade, but with hacking examples growing in news sources like the Wall Street Journal, Washington Post, and New York Times, all of a sudden there is plenty of press on the subject.[45] This is to be expected in a world filled with what Dave Grossman calls sheep, wolves, and sheepdogs. Grossman says the sheep (Society) pretend the wolf (Enemy) will never come, but the sheepdog (Military—defenders of

[44] Winton, "An Imperfect Jewel," *The Journal of Strategic Studies,* 856.

[45] Recent articles that speculate where the cyber-attacks came from can be found in on-line articles. See Nicole Perlroth, "Washington Post Joins List of News Media Hacked by the Chinese," 1 February 2013, http://www.nytimes.com/2013/02/02/technology/washington-posts-joins-list-of-media-hacked-by-the-chinese html?_r=0.

Society) lives for that day; well, that day is already upon the US in regards to cyber war.[46] The question is what is the US going to do about it?

Comments by senior leaders like William Lynn, the US Deputy Secretary of Defense, warn, "If a terrorist group does obtain destructive cyber-weapons, it could strike with little hesitation."[47] Not necessarily a sheepdog, Secretary Lynn is both creating anxiety within cyberspace, a realm the sheep of most societies view as non-threatening. He is also awakening the sheepdog, the military, to problems that have been watched for some time, but one in which an offensive military response has not yet been warranted; and will not be until the sheep support such actions. There is however still challenges to the claim Secretary Lynn makes which prevent a military response short of declared war.

First, the US has not defined what constitutes a cyber-attack. Second, US policy-makers have not publicized what type of cyber-attack upon the US constitutes a military response; either via military cyber capabilities or other US military instrument of power. The second point is important for any USAF cyberpower response, although it does not prevent the service from building capabilities to respond when called upon. The author argues the USAF could however prepare more effectively with objectives defined clearly by the policy-makers. For that reason, defining a cyber-attack that warrants a military response is required.

The rhetoric espoused by Ed Pilkington's piece stating the Obama administration, "will respond to hostile acts [against the US] in cyberspace as we would to any other threat to our country," does nothing to clarify or define a cyber-attack.[48] Neither does publishing books such as *Cyber Attacks* by Edward Amoroso that talk more about potential vulnerabilities of US systems and what steps can be taken to mitigate known

[46] Sheep do not like the sheepdog because they look like the wolf. He has fangs and the capacity for violence. The difference, though, is that the sheepdog must not, cannot and will not ever harm the sheep. Any sheepdog who intentionally harms the lowliest little lamb will be punished and removed. The world cannot work any other way, at least not in a representative democracy or a republic such as ours. This analogy provided by retired Lt Col Grossman mirrors the general public—the sheep—terrorists or aggressive nation states that seek war with the US—wolves—and US military forces, too include any public protective service like local and state police, FBI, and others—sheepdogs. D. Grossman and L.W. Christensen, *On Combat: The Psychology and Phsiology of Deadly Conflict in War and Peace* (PPCT Research Publications, 2007), 182-83.

[47] William Lynn, "The Pentagon's Cyberstrategy: One Year Later," *Foreign Affairs*, (28 September 2011), http://www.foreignaffairs.com/articles/68305/william-j-lynn-iii/the-pentagons-cyberstrategy-one-year-later

[48] Ed Pilkington, "Washington Moves to Classify Cyber-Attacks as Acts of War," *The Guardian*, (31 May 2011), http://www.guardian.co.uk/world/2011/may/31/washington-moves-to-classify-cyber-attacks.

vulnerabilities.[49] To hone a definition of what constitutes a cyber-attack, zeroing in on what is critical to US national security appears relevant. What is also relevant is to acknowledge the fact that it is “the public, the civilian population of the US, and the publicly owned corporations that run our key national systems, that are likely to suffer in a cyber-war;” as Richard Clarke alludes to in *Cyber War*.[50] Clarke’s definition of cyber-war—actions by a nation-state to penetrate another nation’s computers or networks for the purpose of causing damage or disruption—can shape a US definition of cyber-attack; at least in relation to conflict between nation-states.[51]

Turning to the United Nations (UN) there is still no clear standard to what constitutes a cyber-attack. No formal definition exists. However, evaluating the UN charter leads to the conclusion that the use of force would include cyber-attacks since it is a domain for warfare just as is air, land, sea, or space.[52] Article 51 of the UN Charter allows for the right of self-defense, however, ruling by the International Court of Justice have set a high bar to exercise the right.[53] Many cyber actions may not meet the ICJ standard; however, Article 39 of Chapter VII states the UN Security Council “shall determine the existence of any threat to peace, breach of the peace, or act of aggression and make a recommendation.”[54] Any recommendation the Security Council makes falls under Articles 41 and 42 of the charter. Article 41 covers non-military responses,

[49] For a guide to improve existing infrastructure components or build new ones, see Amoroso, *Cyber Attacks: Protecting National Infrastructure*: 9-11.

[50] Clarke and Knake, *Cyber War: The Next Threat to National Security and What to Do About It*: xiii.

[51] Clarke and Knake, *Cyber War: The Next Threat to National Security and What to Do About It*: 6.

[52] UN Charter Article 2(4).

[53] The ICJ in US vs. Nicaragua discussed the right of self-defense, “The general rule prohibiting force established in customary law allows for certain exceptions. The exception of the right of individual or collective self-defense is also, in the view of States, established in customary law, as is apparent for example from the terms of Article 51 of the United Nations Charter, which refers to an "inherent right", and from the declaration in resolution 2625 (XXV).” . . . Whether self-defense be individual or collective, it can only be exercised in response to an "armed attack". In the view of the Court, this is to be understood as meaning not merely action by regular armed forces across an international border, but also the sending by a State of armed bands on to the territory of another State, if such an operation, because of its scale and effects, would have been classified as an armed attack had it been carried out by regular armed forces.” However the court stated, “States do not have a right of "collective" armed response to acts which do not constitute an ‘armed attack’.” Case Concerning the Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America) 27 June 1986, UCJ Section X 2. http://www.icj-cij.org/docket/?sum=367&code=nus&p1=3&p2=3&case=70&k=66&p3=5.

[54] To read specifics on United Nations and Security Council actions see the United Nations Charter, Chapter VII, Article 39, http://www.un.org/en/documents/charter/chapter7.shtml.

whereas Article 42 allows military response in the form of land, air, or sea forces.[55] Thus, the door is open for a potential military response to another country's aggression via cyber-attack.

A nation claiming to be harmed by a cyber-attack by another nation-state that did not rise to the level of an armed attack could make their claim to the UN. The UN Security Council would evaluate such a claim and determine if a use of force response is warranted, just as it currently does for the other three authorized warfare domains—air, land, and sea. Using inductive reasoning, and because the UN charter has yet to include cyber-war, or defined what constitutes a cyber-attack, we can add 'cyber' as a domain in which a response under Article 42 or 51 can be conducted. But we still do not have a clear standard as to what constitutes a cyber-attack. Nor does the speed at which cyber-attacks occur allow for the time needed to gain approval from the UN in order to quickly respond.

It is safe to presume, based on every war or conflict that has concluded since the UN was founded in 1945, a legal review will occur by the UN for each war.[56] Lawyers will review actions before war—*Jus ad Bellum*—as well as actions in war— *Jus in Bello*.[57] In pursuit of a usable definition of a cyber-attack that would constitute an act of war, therefore *Jus ad Bellum*, we turn to circulated literature regarding cyber-attack in the legal realm. Matthew Waxman in the *Yale Journal of International Law* provides a starting point. Matthew defines cyber-attacks as, "efforts to alter, disrupt, or destroy computer systems or networks or the information or programs on them…encompassing activities that range in target (military versus civilian, public versus private), consequences (minor versus major, direct versus indirect), and duration (temporary versus long-term)."[58]

[55] United Nations Charter, http://www.un.org/en/documents/charter/chapter7.shtml.

[56] See information regarding the founding of the United Nations at: http://www.un.org/en/documents/charter/intro.shtml.

[57] *Jus ad Bellum* discusses actions leading up to war to aid in determining if actions before war made the act of going to war *just*. *Jus in Bello* evaluates actions in war to determine if war was conducted in a *just* way. For additional details on both *Jus ad Bellum* and *Jus in Bello*, see P.M. Walzer, *Just And Unjust Wars: A Moral Argument With Historical Illustrations* (BasicBooks, 2006).

[58] For an exceptional well discourse regarding cyber-attacks and the challenges facing the US and international community alike surrounding this issue, see Matthew Waxman, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)," *Yale Journal of International Law*, V 36:2 (Fall 2010), 421-459, at http://www.yjil.org/docs/pub/36-2-waxman-cyber-attacks-and-the-use-of-force.pdf. Also see the

Accepting this definition of a cyber-attack, the target of a cyber-attack has endless possibilities given the pervasive interoperability between cyberspace and countless operations conducted within society each day, not to mention the differing nefarious actors conducting cyber-attacks. Since the scope of possible targets for cyber-attack within the US is much too broad for US military forces to focus on, even excluding the challenges of the appropriate authorities governing law enforcement forces, federal agency services, and the military discussed in chapter 4, it is important to focus on threats to US national security for our discussion and theory development.[59]

Interests involving national security can be derived from published grand strategy guidance such as the National Security Strategy. The National Security Strategy, signed by President Obama in 2010, is currently what the US employs to inform the international community of its interests.[60] Dissecting the current security strategy, there are four enduring national interests:

1. **Security:** The Security of the United States, its citizens, and the US allies and partners
2. **Prosperity:** A strong, innovative, and growing US economy in an open international economic system that promotes opportunity and prosperity
3. **Values:** Respect for universal values at home and around the world
4. **International Order:** An international order advanced by US leadership that promotes peace, security, and opportunity through stronger cooperation to meet global challenges[61]

Breaking the National Security Strategy down to a focus of AF cyberspace operations, since that is the focus of this treatise, requires a look at the AF vision intended to meet defined national objectives. The recently appointed Chief of Staff of the Air Force provided such a vision. General Welsh described five roles and responsibilities

definition of cyber attack in Tallinn Manual on the International Law Applicable to Cyber Warfare, Micaheal N. Schmitt (ed), New York: Cambridge University Press, (2013) at 106.

[59] The USAF developed a bullet background paper on US code-based authorities relevant to cyber operations. It is an unclassified paper but accessed through authorized Air Force headquarters organizations. Title 6—domestic security—Title 10—Armed Forces—Title 18—Crimes and Criminal Procedure—Title 32—National Guard—Title 40—Public Buildings, property, and Works—Title 50—War and National Defense are all discussed relative to cyber. The unpublished bullet background paper provided via Headquarters Air Force Sharepoint site.

[60] See the National Security Archives for existing and past National Security Strategies, http://nssarchive.us/

[61] For specific details regarding US national security see the *National Security Strategy* (May 2010), 17, http://www.whitehouse.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

inherent since 1947 when the AF was founded as today's AF vision: air and space superiority; intelligence, surveillance, and reconnaissance; rapid global mobility; global strike; and command and control.[62] Making one addition to the first role and responsibility in the CSAF's vision, a change now reads 'air, space, and *cyberspace* superiority' to include the three primary roles defined in the AF mission of "Fly, Fight, and Win in Air, Space, and Cyberspace."[63] This is also in line with the Fiscal Year 2013 Air Force Posture Statement published in early 2012.[64]

A review of the AF posture statement leads to a second change in the current vision by General Welsh; the author adds 'Nuclear Deterrence' as a sixth primary role and responsibility. There are additional focus areas within the posture statement that are important to national security and susceptible to cyber-attacks, but limiting this treatise to developing an AF cyberpower targeting theory, the author chose to limit his focus to six primary roles and responsibilities. If these are six areas the Air Force decides are critical to Airpower operations and should be protected from an adversary's cyberpower capabilities, we can inversely say these may be enemy centers of gravity to exploit—presuming the adversary is a peer competitor with the US.[65] Accepting this inference keeps with the advocacy of Clausewitz and Warden's principles of defining enemy and friendly centers of gravity before war.

[62] Read the full vision of General Mark Welsh III, "A Vision for the United States Air Force," http://www.af mil/shared/media/document/AFD-130110-114.pdf.

[63] United States Air Force, "2013 Air Force Mission Statement," http://www.posturestatement.af.mil/main/welcome.asp.

[64] Read the presentation to the Committee on Armed Services United States House of Representatives, presented as the "United States Air Force Posture Statement 2012," http://www.afa.org/PresidentsCorner/WashingtonPerspective/2012/02282012_HASC_USAF_Joint_Statement.pdf.

[65] Before this list is final, the Air Force should clearly define what air, space, and cyberspace superiority is. Once defined, a determination should be made as to whether or not each objective is achievable or desired. Specifically, if cyberspace superiority is having the ability to operate in a contested cyberspace environment, that may be achievable. If cyberspace superiority is controlling the entire cyberspace, that may be an unattainable, or even desired, objective.

Table 13

Six Air Force Cyberpower Targeting Roles

air, space, and cyberspace superiority
intelligence, surveillance, and reconnaissance
rapid global mobility
global strike
command and control
Nuclear Deterrence

Source: Author based on published documents

Categorize

With cyber-attack clearly defined, and the six critical capabilities levied upon the USAF to both protect defined national security vulnerabilities, as well as project military power in support of national security interests, we have derived six definitive cyberpower targets. These targets will shape Air Force cyber operations in the form of offensive, defensive, and exploitation initiatives.

From an offensive and defensive perspective, USAF cyber-forces must conduct both active and passive operations in both realms to prevent adversary attempts to alter, disrupt, or destroy any computer system, network, information, or software program associated with the six defined roles and responsibilities. These efforts require coordination with other military services, civilian agencies, and allies in order to guarantee the capability of each Air Force mission. On-going cyber exploitation initiatives during peacetime and war are necessary to ensure cyberspace freedom to maneuver exists when needed.

In order to deter adversary aggression in these areas, it is recommended that US policy-makers establish policy stating that any cyber-attack on these assigned Air Force roles and responsibilities will be considered an act of aggression. This same policy effort should be done for all areas of national security interests; however, the focus remains on the Air Force for this treatise. The policy should also state that cyber-attacks deemed acts of aggression will be met with an immediate response by the appropriate instrument of power as determined by policy-makers. Publishing this policy would be a first step in establishing both domestic and international standards, or code of conduct, within cyberspace and potentially act as a deterrent.

Establishing a defined policy regarding cyber-attack, in addition to the already stated AF mission of cyber superiority, also enables the creation of cyber-targets for offensive cyber operations. Reflecting on what the AF deems critical to mission success, an inverse look at similar capabilities of an adversary identifies potential centers of gravity for cyber-attack by US forces. Finding, fixing, tracking, targeting, engaging, and assessing roles are just as critical in cyberspace operations as they are in land, air, and sea warfare. If anything, cyberspace operations require more intelligence gathering and verified updates than any other domain with the higher probability of being wrong. This is due to the expedience in which this man-made domain changes compared to other domains.

General Shwedo, Director of Intelligence, Headquarters Air Combat Command, says, "Cyber is an Intel hog."[66] His point hinges on a few key differences regarding intelligence gathering, consolidation, processing, and then supporting on-going and future operations. General Shwedo acknowledges the well-known "Observe, Orient, Decide, Act" (OODA) loop of Colonel John Boyd and postulates Boyd's loop is defined as an "Operate, Attack, Exploit, Defend" loop in cyber operations.[67] This loop is applicable in offensive, defensive, and exploitation objectives of AF cyber-operators. While attempting to define each capability it is important to call upon the renowned Prussian.

Clausewitz states that the characteristic of war may be split into two main categories: preparations for war and war proper.[68] Agreeing with this premise, the author equates offensive and defensive cyber operations as primarily war proper activities with some aspects conducted during preparations for war; whereas cyber exploitation is a

[66] This quote is from an interview conducted by the author. Brigadier General Brad "BJ" Shwedo, interview by author, Maxwell AFB, AL., 2 November 2012.

[67] Most of Colonel John Boyd's information surrounding his OODA loop exists in presentation format and not a published book by Colonel Boyd. For a synthesis of his works see F.P. Osinga, *Science, Strategy and War: The Strategic Theory of John Boyd* (Taylor & Francis, 2007).

[68] Clausewitz, Howard, and Paret, *On War*: 131.

preparation for war activity with some aspects conducted during war proper. It is also important to point out a contrary point to Clausewitz here. Clausewitz says "defense is the stronger form of combat."[69] His point is relative to maintaining the physical forces of a country for if those forces are lost then the country is lost automatically. This is not the case with cyber-operations. Martin Libicki substantiates why offensive cyber forces must be engaged actively and active adversarial capabilities destroyed, disabled, or otherwise inhibited.[70] He posits, "In cyber, offense is cheap and can have disproportionately great effects at the levels of attack—advantage attacker.[71] Therefore, offensive cyberpower is vital.

Offensive cyber operations are arguably the strongest form of warfare in cyberspace. Given the diverse nature of cyberspace and the resilience in which it allows operations to rapidly move from one location to the next, cyberwarfare is a cunning tool in war. Unless you can remove the true genius of its ability—the human operator—the defensive battle as the stronger form of warfare Clausewitz advocates appears incompatible with the cyberspace domain. Offensive operations, both non-kinetic and kinetic must be the priority for cyber operations. Depleting aircraft, aircraft carriers, tanks, and even soldiers can aid in determining an adversary's warfighting capabilities. Determining where the shadowy cyber-forces are operating makes it difficult to destroy the true capability of cyberpower. The complexity of operating in this domain, under the current incoherent policies governing military operations is evidenced in the fight against Al Qaeda, and is foreshadowing of what is ahead in the battle for cyberspace. In 2010, General Abizaid concluded that in the war against Al Qaeda, "cyberspace is a domain of war where you have to conduct defensive and offensive operations. The enemy was moving in the cyberspace world in a way that allowed them to recruit, train, organize, equip, proselytize, educate, and conduct intelligence operations."[72] For a force that can

[69] Clausewitz, Howard, and Paret, *On War*: 484.

[70] The use of "active adversarial capabilities" alludes to a similar meaning Secretary of Defense Cohen noted in his memorandum to US military leaders regarding a new DOD Space Policy in 1999. The point is any direct action against US assets will be considered an act of aggression against the US. Secretary Cohen said that "purposeful interference with US space systems will be viewed as an infringement on our sovereign rights." John Donnelly, "Cohen: Attack on US Satellite Is Attack on United States," *Defense Week*, 26 July 1999, 2.

[71] Libicki, *Cyberdeterrence and Cyberwar*: 33.

[72] E. Schmitt and T. Shanker, *Counterstrike: The Untold Story of America's Secret Campaign Against Al Qaeda* (Henry Holt and Company, 2011), 135.

literally operate around the globe instantaneously, this makes cyber warfare that much more complex than any other warfighting domain.

This is a clear delineation between the cyber domain and the other warfighting domains. Knowing the enemy's offensive disposition in cyber is virtually impossible. Even if a lack of enemy capabilities exists before war begins, once war starts intelligence can quickly assess how many ships, airplanes, and even fighting forces in brigade formation an adversary has. This is not easily identifiable in cyberspace. This is exactly why offensive cyber operations cannot be relegated to tit-for-tat operations, or be used solely as combat air support for fielded forces as airpower was originally; this type of action places military operations back in attrition style of warfare. This is also why military cyber forces should focus more on offensive operations rather than defensive; at least on the spectrum of war continuum.

Offensive cyber can assist air, land, sea, and space forces in achieving their operational requirements. But, to be the most effective, offensive cyber should be used to target strategic capabilities that aid political objectives to bring about quick conflict resolution. Employing Warden's model of the enemy as a system and targeting national command and control capabilities, key processes, infrastructure, the population, and fielded forces, seems to be the most efficient method in which to employ cyberpower; at least theoretically. DOD and specifically AF cyber forces must be prepared to conduct simultaneous offensive cyber operations targeting each center of gravity of the enemy's systems. Obviously these efforts must coordinate actions with those in other domains to ensure synergy is achieved. However, there is little doubt that cyber will be the first salvo fired in future wars.[73]

Cyber defense is arguably conceptually different than other warfare domains. The US has a Navy to defend the littoral territorial boundaries; air defenses, either through missile defense initiatives or alert aircraft both have defined airspace boundaries; but in cyberspace those lines are not readily identifiable. Susan Brenner acknowledges

[73] Nations around the world are expanding their cyber forces and growing capabilities, despite shrinking defense budgets. The United States is doing the same. When countries like Israel threaten pre-emptive strikes against an adversary that include cyber-attacks on command-and-control networks, and communications and infrastructure to degrade military capabilities, it is clear cyber-power projection will occur at the earliest stages of warfare. United Press International, "Israel Builds up its Cyberwar Corps," 2 November 2012, http://www.upi.com/Business_News/Security-Industry/2012/11/02/Israel-builds-up-its-cyberwar-corps/UPI-52421351881449.

traditional attacks from the territory of one nation-state upon the sovereign of another presumptively constituted an act of war.[74] She goes on to say the contemporary territorial boundaries are antiquated parameters in determining cyber-threats. The question is why? People still reside in a sovereignty and if a cyber-threat affected a society in the sovereignty in which they live, no matter what form or domain an attack originates, why treat it any differently? Until the international community develops a standard for cyber-threat resolution, a formal US policy is warranted that states US intentions to respond to cyber-threats serves as the applicable law and warning. Such a law should apply to US citizens living within the territorial boundaries of the US; as well as non-US citizens living within the US borders. Those who break the stated laws should pay the consequences. This is no different than domestic laws such as speeds. Either people respect them and avoid penalty and punishment or they choose to disobey them and are subject to applicable consequences.

Defensive cyber operations appear to be the primary focus of AF cyber operations today. This same effort is pervasive across DOD and civilian cyber efforts as well. From automated host base security system efforts that report vulnerabilities through automated scripts to passive defense protocols to ensuring the latest anti-virus software is loaded on government computers, these are all very costly efforts to keep up. In reality, they are all reactive security measures that do little more than provide a false sense of security to the average user of cyberspace. They are useful, but only up to a point.

Zero-day exploits by those who initiate cyber-attacks are not deterred by signature based anti-virus software programs, which is what today's anti-virus software updates are based on.[75] Attackers know it will take on average up to nine months or more before any new virus protection will identify the exploit they create, and then it is incumbent on software owners to actually get the software updates to close the vulnerabilities; something that does not occur automatically.[76] That allows for a lot of maneuverability

[74] S.W. Brenner, *Cyberthreats: The Emerging Fault Lines of the Nation State* (Oxford University Press, 2009), 81.

[75] A zero-day cyber-attack is an unknown exploit which proliferates throughout cyberspace to which no known defenses initially exists. The Conflicker worm is an example of a zero-day exploit which to some observers was known as a "digital blitzkrieg." Bowden, *Worm: The First Digital World War*: 1-23.

[76] There is malware available on the open market that offers a "service level agreement and replacement warranty if the purchased malware is detected by any anti-virus software within nine months." This affirms that those who employ malware do not perceive a threat from anti-virus software for at least nine months.

in cyberspace for an adversary. The damage sought is most likely done within nine months of an attack, or additional unknown vulnerabilities planted in other cyber systems which can be executed at the adversaries choosing.[77] These are the same attackers who are actively seeking software vulnerabilities and creating "logic bombs" to exploit vulnerabilities without being detected.[78] They are well versed when anti-virus script updates occur and which vulnerabilities have been closed.

Given the unlimited vulnerabilities to DOD networks, and the fact that the DOD does not own their own infrastructure, develop their own software programs that govern all military needs, or provide maintenance for their end-to-end cyber systems that support defined national security objectives, a change in DOD and specifically AF defensive cyber operations is required. The focus must shift from trying to protect all AF and DOD cyberspace to one that guarantees protection of the cyberspace that is critical for national defense and national security strategic objectives. In other words, the six roles of AF cyberpower targeting defined above become the primary focus of AF cyber defense operations for cyber-forces. The primary job of Air Force cyber-forces is to conduct relentless protection of those capabilities to assure mission success when these capabilities are called upon.

The proposed concept might push militaries to operate in two distinct cyberspace domains—open versus closed—for both security and operational reasons. Zimmet and Barry argue there are two broad cyberspace regimes which require different attributes. The first is an open network that aids collaboration, information-sharing, and situational

John Suffolk, "Cyber Security Perspectives," *Huawei*, September 2012, 10, http://www.huawei.com/ilink/en/download/HW_187368.

[77] Additional inferences regarding network detections taking an extended period can be seen in comments by General Alexander, commander of US Cyber Command and director of the National Security Agency. He stated "that when people break into a network, they're often there for six to nine months before we detect them." While in the network, the attackers "own the networks" for that time and have the ability to take whatever they want. Cameron Cox, "NSA Director on Cyberattacks: 'Everybody's' Getting Hit," *ABC News Radio*, 7 November 2012, http://abcnewsradioonline.com/business-news/tag/hackers.

[78] Logic bombs are a set of instructions that are intentionally designed to execute when a particular condition has been satisfied. Commonly these bombs delete or corrupt data, reset passwords, or have other harmful effects. These malicious programs can be introduced through a variety of means, months or even years before they need to be triggered for a specific operation. John Bumgarner, "Computers as Weapons of War," *IO Journal* (May 2010): 6, http://www.nxtbook.com/nxtbooks/naylor/JEDQ0210/index.php?startid=4#/4.

awareness.[79] The second is a closed, secure network in which speed of operation, assured delivery, and integrity of information are vital.[80] As an experienced cyberspace operator, the closed network is most appealing for mission assurance. However, military forces must also operate in the open network to interact and collaborate with allies and exploit adversary vulnerabilities. Military commanders must advocate the right balance based on cost/benefit analysis and acceptable risk tolerance between mission assurance and offensive and exploitation actions in a contested cyberspace.

The last category for AF cyberspace operations is exploitation. Authors such as Thomas Rid of King's College London argue "cyber war will not take place."[81] In addition to stating cyber war has never happened and it is highly unlikely it will occur in the future, Rid argues sabotage, espionage, and subversion are not cause for war. This fallacy is based on the lack of defined nation-state policy and established international laws. This author's argument is that once the US defines such acts as illegal, they do become acts of aggression which can lead to war. However, there does need to be some common sense in this approach. The author delineates actions conducted in open-source cyberspace—information found searching around unprotected or inadvertently made public is fair game and is not illegal—compared to closed network systems—circumventing security protections or hacking into non-open-source systems—leaves room for espionage type activities. This is no different than human intelligence activities that gather information through social engineering or observation techniques.

These open source activities are not to be misconstrued with active deceit. Exploiting the weakest part of the infrastructure—the people—by sending an email phishing exploit with an embedded executable file would be considered an act of low-threat aggression.[82] However, requesting users to complete on-line surveys or other persuasion techniques to get users to relay information would not be. Any user who

[79] Elihu Zimet and Charles Barry, "Military Service Overview," in Kramer, Starr, and Wentz, *Cyberpower and National Security*: 288.

[80] Elihu Zimet and Charles Barry, "Military Service Overview," in Kramer, Starr, and Wentz, *Cyberpower and National Security*: 288.

[81] Thomas Rid, "Cyber War Will Not Take Place," *Journal of Strategic Studies* 35, no. 1 (February 2012): 6, http://dxdoi.org/10.1080/01402390.2011.608939.

[82] For an understanding of vulnerabilities surrounding cyberspace and social engineering tactics currently being employed in cyberspace, see C. Hadnagy, *Social Engineering: The Art of Human Hacking* (John Wiley & Sons, 2010), 2.

knowingly provides sensitive information would constitute a failure of internal processes, procedures, and training.

Exploitation efforts require enormous intelligence gathering resources to help shape the cyber operators focus. The starting point for exploitation efforts would be equivalent adversary capabilities for the six Air Force cyberpower targeting roles identified earlier. From there, defined centers of gravity of a potential adversary in regards to cyberspace reliance would shape US espionage efforts. Any function that supports the enemy's strategic systems would invariably become exploit areas of interest. Understanding the inter-connectedness of the systems, vulnerabilities at choke points where data flows, reliance on consolidated power sources, or cloud data storage facilities, intelligence collaboration centers, or combined area processing centers for logistics, banking, agricultural, or other societal dependent functions also become critical. These exploitation efforts must be constantly coordinated with offensive and defensive actions within military agencies and non-military agencies alike to ensure redundancy and waste are avoided, as well as, synchronized efforts toward a target in order to not cause fratricide to friendly cyber operations.

Explain

As mentioned several times throughout this thesis, the military is one instrument of national power; one that serves the political objectives of policy-makers. For that reason, military commanders are constantly aware of threats to national security that presumably many members of society either do not notice or choose to ignore. Recall the sheep discussion from Grossman earlier. So, until societies realizes a threat and push elected officials to resolve those threats, military and other federal agencies are limited in threat response actions. Responding to cyber-threats is no different.

In 2012 Congress lobbied for legislation that would allow the National Security Agency to share its sophisticated cyber-security tools with the corporate sector; that legislation was opposed by the US Chamber of Commerce.[83] Now in early 2013, after an onslaught of "distributed-denial-of-service attacks," and new "swarm" attacks on "the

[83] 'Botnets' Run Wild, *Washington Post*, 24 January 2013, as found in the Early Bird through authorized access: http://www.news-herald.com/articles/2013/01/24/opinion/nh6474510.txt.

soft underbelly of American society," the private sector is requesting government help to thwart recent attacks.[84] It appears both an opportunity for the civilian sector to strengthen their cyber-security capabilities, and military and other federal agencies to test offensive and defensive capabilities to counter growing threats. It is also a prime time for policy-makers to establish acceptable cyberspace behavior standards before too many more precedence are set by not condoning or responding to cyber threats.

Operating in the vulnerable sectors of a nation's cyberspace, before war is declared, can be considered phase-zero military operations. Without delving into tactical offensive, defensive, or exploitation specifics, explaining each phase of military operations invites critical thinking about when and how cyber effects might be employed.

Pundits argue "phase-zero" is new to the military lexicon whereas phase 1 to phase 5 operations are traditional military roles substantiated in existing doctrine.[85] This may have been true years ago, but it is an antiquated argument today. Turning to joint doctrine for an understanding, Joint Publication 3-0, *Joint Operations*, shows clearly six phases of military operations. Figure 3 below is an excerpt from the publication and succinctly captures traditional military endeavors during each phase.

[84] 'Botnets' Run Wild, Washington Post, 24 January 2013, as found in the Early Bird through authorized access: http://www.news-herald.com/articles/2013/01/24/opinion/nh6474510.txt.
[85] Center for Global Development, "Phase Zero: The Pentagon's Latest Big Idea," 20 July 2007, http://blogs.cgdev.org/globaldevelopment/2007/07/phase-zero-the-pentagons-lates.php.

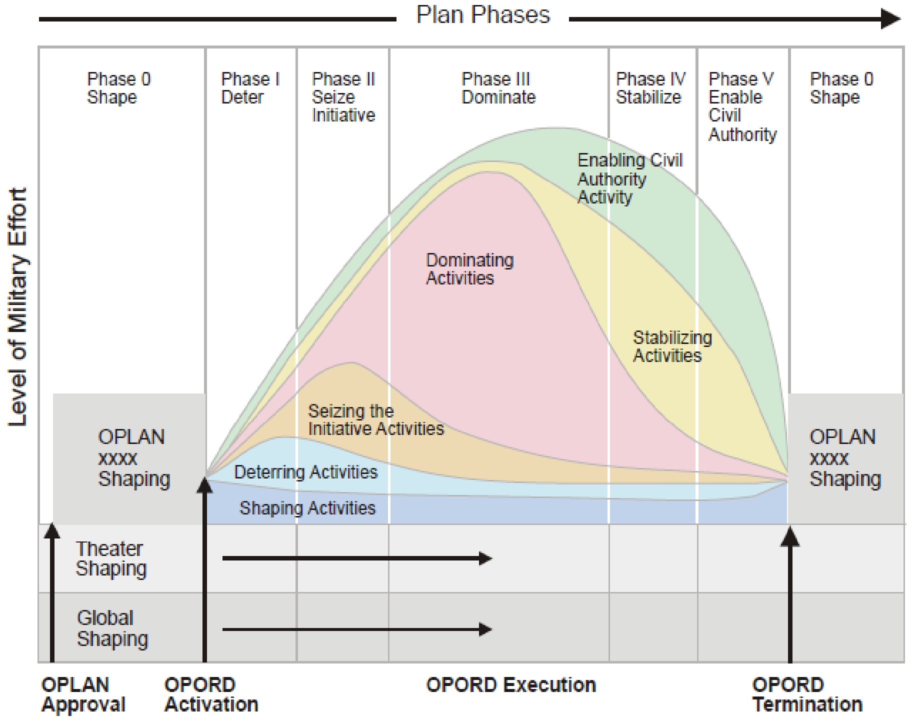


Figure 3: Military Phases of Operation
(Source: *Joint Publication 3-0*, Figure V-3. Notional Operation Plan Phases)

The author suggests shaping operations in cyberspace are on-going throughout the entire pendulum of peace and war, and back to peace again. Advocating this position is not intended to suggest that aggressive military operations in cyberspace are always required during times of peace, but rather the intent is to suggest that shaping the cyberspace sphere inevitably occurs in peace since cyberspace is a constantly restructured domain constructed by man-made efforts to influence the electromagnetic spectrum. Therefore, it is reasonable to presume that shaping and deterring efforts in cyberspace through offensive, defensive, and exploitation efforts, which are categorized traditionally as Phase-1 operations for traditional warfighting domains, will occur in Phase-0. This is also where cyber capabilities can have strategic impacts by shaping these phases through "influence operations" in a manner in which cyberpower has not previously been used.[86]

[86] Colonel Paul Welch is the current commander of the 688th Information Operations Wing, Lackland AFB, TX. During a telephone interview he suggested that traditional Air Force roles of Compass Call or air drops of leaflets during phase 1 and earlier operations may have to change in order to gain full effects afforded by cyberspace. He goes on to say that "maneuver through the domain requires constant attention through and to the target. There are four areas we must focus on: target selection is complex, maneuver to the target and having the ability to have a technical affect is required, determine if the effect what we are looking for, and how can I assess the result?" Colonel Welch affirmed that cyber-power capabilities must

If this observation is an accepted truth, then it is incumbent on policy-makers and military forces alike to use national treasures to prepare now for cyber warfare in future conflicts and war. This preparation comes with organizing, training, and equipping a force to conduct independent or supporting operations while defining what roles other warfighting domains might play in supporting cyber operations. This is not the first time the US has been at a decision point regarding building support for a new warfighting capability.

Unlike the interwar years when the US appropriated "no investment to original research and development" of aircraft, today's national and defense appropriations are directly focused on enhancing cyberspace operations.[87] Now is the time to capitalize on defining the centers of gravity of potential nation-state adversaries, exploiting the vulnerabilities to a cost/benefit level acceptable by military commanders and politicians alike, while developing state-of-the-art offensive cyber weapons and using them when stated policy regarding acceptable cyber behavior is violated.[88]

Organizing, training, and equipping cyber forces are crystal clear when defined objectives are known to military commanders. Knowing that offensive forces are the primary objective, followed by defensive and exploitation forces establishes priorities for sizing and organizing forces for each needed capability. These priorities also shape weapon system procurement by focusing on offensive tool research, development, creation, and testing of capabilities to achieve desired objectives; followed by tool development for defense and exploitation. Finally, equipping the force to meet their stated objectives is the product of following the defined strategy.

By defining what is needed to equip a force capable of achieving defined objectives contributes directly to the training needed. To put it in simple terms, if new technologies are needed to support offensive operations and those tools require internal

provide "a variety of options to COCOMS," just as all warfighting domains should, but that cyber capabilities should not be confined and prevented from achieving its full potential. Colonel Paul Welch, (688 IOW/CC), telephone interview by author, 12 December 2012.

[87] De Seversky, *Victory through air power*: 218.

[88] At a time when the US defense budget is shrinking across most major weapon systems, USCYBERCOM and service specific funding requests for cyber operations were approved and in some cases saw an increase in funding. This is a clear message that cyberspace threats are starting to be recognized as detrimental to national security interests. For specifics on US defense spending surrounding cyberspace, see the 2013 National Defense Authorization Act, "One Hundred Twelfth Congress of the United States," 3 January 2012, http://www.gpo.gov/fdsys/pkg/BILLS-112hr4310enr/pdf/BILLS-112hr4310enr.pdf.

development for security or secrecy reasons, then software engineers may be deemed critical to mission success. However, if remote "gap jumping" technology is needed, along with Airmen skilled in creating the mobile cyberspace environment—known as cyber-extension to some—then training is required to meet those specific needs.[89] When mission needs are driven by defined roles, then focused efforts on recruiting, training, and equipping the right cyber-force becomes less arbitrary and more deliberate. This leads to the third byproduct of defined targets for Air Force cyber-effects; organizing the force.

The Air Force does not own cyberspace, not even the cyberspace for its six defined roles described above. Whether or not the Air Force pursues a "closed" network for mission critical roles, or pursues functional capability in the "open" network, collaboration with other military services, federal agencies, and the civilian/commercial cyberspace community is necessary. However, given the inter-connectedness of cyber operations throughout practically all critical national security interests, does it make more sense to create a consolidated national cyber-force where entities from military, federal, and civilian/commercial industry operate under one authority? This is not intended to mandate oversight of cyberspace by the government; governance of rules and compliance mandates would only apply to areas of cyberspace that directly relate to national security.

Although outside the scope of this treatise, a quick observation of other nation-states might highlight efforts that create more cyberspace efficacy than current US efforts. This thought is driven by the growing number of legislative proposals to increase cyber-security within the US that undoubtedly go unheeded for various reasons. First, most commercial businesses and individuals throughout society are not inclined to spend their money to close cyber-security vulnerabilities that have not affected them. They might believe that if the government wanted them fixed, they would pay for them. Second, there might be a belief that current policy and practices regarding cyber-security are outdated. If the government were to hold the creators and distributors of software accountable for errors in programming code, which is where many known cyber-security vulnerabilities proliferate, then those manufacturers should be required to 'push' software

[89] The term cyber-extension is sometimes used in mobile communications circles like combat communications. Cyber-extension refers to the ability to bring cyberspace to a place it currently did not exist through deployable mobile assets that enable connection to cybespace with mobile satellites, switches, and routers in order to connect to the global information grid.

updates to all users free of charge. This would eliminate the individual and corporate expenses of anti-virus software and it would drive better software development before the release of a product. It would also put ownership of the vulnerability resolution where it belongs; with its creator.

A simple analogy to this thought can be seen in the auto-industry. When a safety fault is found in a vehicle, the manufacturer is responsible for notifying owners as well as paying for the repair. There is no reason this process could not work in cyberspace. If the vulnerabilities are truly a security threat, then software manufacturers should be responsible for resolution without relying on the end-user. Unlike the car manufacturing scenario, an automated software patch could be pushed globally and the next time the system interacts with the Internet, it receives the fix automatically.

Getting back to the make-up of cyberspace organizations, looking at Australia's activities provides a potential organizational structure that consolidates a nation's interests regarding cyberspace operations and their desired security regarding those interests. Taking this approach not only affirms cyberspace as an independent capability requiring an independent force to address its highly technical needs, but eliminates redundancy that inevitably occurs when various forces and organizations develop the same training and equipping needs, not to mention additional overhead in running various cyber-forces throughout diverse military forces and civilian agencies.

Australia declares, "Our national security is the most basic expression of our sovereignty…and national security is the most fundamental task of government." Specific tasks assigned to the Australian government are identified in the 2013 National Security Strategy.[90] Of three specific tasks the Australian government is dedicated to over the next five years, "identify[ing] area[s] for increased effort in cyber security," is the second task.[91] To achieve this monumental task, the Prime Minister, Julia Gillard, not only established an Office of the Cyber Policy Coordinator to provide leadership and coordination on important cyber issues, but she envisioned a new Australian Cyber

[90] The author is indebted to his Australian counterpart in SAASS Class XXII, Squadron Leader Travis Hallen, for bringing this document to his attention. To read the full article detailing Australia's national security strategy, see "Australia's National Security Beyond the 9/11 Decade," http://www.pm.gov.au/press-office/australias-national-security-beyond-911-decade.

[91] See "Australia's National Security Beyond the 9/11 Decade," http://www.pm.gov.au/press-office/australias-national-security-beyond-911-decade.

Security Centre. The Centre is intended to be "a world-class facility combining existing cyber security capabilities across the Attorney-General's Department, Defense, ASIO, the Australian Federal Police, and the Australian Crime Commission in a single location."[92]

Consolidating efforts, as Australia intends, not only enables a more agile response to government or industry cyber-crime and cyber-security, it also creates a hub for greater collaboration amongst private sector, state and territory governments, and international partners to combat the full breadth of cyber threats.[93] In other words, Australia has recognized cyber-threats as a national issue and is combining all required private, public, and government sectors under one organization in order to create efficacy in addressing cyberspace challenges. In *Airpower for Strategic Effect,* Colin Gray supports an independent service position when he advocates that, "an organization dedicated to cyberpower is likely to advance understanding and capability" of cyber forces."[94] If the US were to take this approach, would it resolve known constraints in conducting offensive, defensive, or exploitation efforts in cyberspace by bringing various national agencies under the purview of one responsible agent? Would this structure create a national cyber-force that not only has the legitimacy to operate on the nation's behalf, but the authority and ability to quickly respond to perceived threats? Would a quick and consistent response increase the US cyber-force credibility across the globe and thus act as a deterrent?

All of these are questions for discussion and further analysis. Even if the US does not pursue a consolidated "Department of Cyber" at this time, it is worth watching other nations who travel this path and conduct not only cost/benefit analysis of such a venture, but monitor cyber-threats and vulnerabilities within those nations to determine if the threat trends rise or fall.[95] Of course, this passive measure of watching other nations create a required cyber-force structure to address national security vulnerabilities resembles watching other nations develop separate air services during the Interwar

[92] See "Australia's National Security Beyond the 9/11 Decade," http://www.pm.gov.au/press-office/australias-national-security-beyond-911-decade.

[93] See "Australia's National Security Beyond the 9/11 Decade," http://www.pm.gov.au/press-office/australias-national-security-beyond-911-decade.

[94] C.S. Gray and B.S. Lambeth, *Airpower for Strategic Effect* (Military Studies Press, 2012): 300.

[95] Department of Cyber is the author's term for what the US might create by combining public and government forces together to protect national security interests regarding cyber and conduct the full spectrum of cyber operations on behalf of the US in both the domestic and international cyberspace.

period.[96] Is there a lesson to be learned from being passive during early airpower development? More directly, is there a lesson to be learned from the early pursuits of airpower in that to truly exploit airpower a nation requires strategic thinkers for the domain independent of constraints to other warfare domains? Billy Mitchell highlighted this pursuit regarding airpower when he said, “The time has come when aviation must be developed for aviation’s sake and not as an auxiliary to other existing branches.”[97] With this in mind, it is valid for future study to examine the question of whether or not cyberpower requires an independent arm to project national power led by those who understand and can develop its full potentials in, through, and from the cyberspace domain. This pursuit will by no means diminish a requirement for the nation’s other military forces to employ cyberpower capabilities to advance effectiveness and efficiency within each warfare domain.

Connect

Developing a cyberpower targeting theory draws upon the same lesson as Clausewitz regarding the violence of war as another means for political intercourse; cyber war is a continuation of this traditional interlude. Therefore, it is important to show how US cyber war is aided by connecting the six defined Air Force cyber-targeting roles to the three ascribed cyber warfare roles—offense, defense, and exploitation—to the phases of war in joint publication 3-0 while correlating applicable principles of war in each phase. Remembering that this approach is theoretical and not prescriptive, the intent is not to create a “strategic bombing theory” such as the ACTS developed and US forces ascribed to in World War II. It is intended to initiate a dialog and suggest potential testing parameters to determine what works, what does not, and if other principles of war are required to effectively conduct a cyber war. These efforts might be described as *Propositions for Cyberpower Targeting*.

[96] Following the Second Balkan War which ended in 1913, many nations recognized the importance of the air weapon and began creating independent air services for national defense. The Royal Flying Corps (April 1012), the Direction de l’Aeronautique Militaire in France (April 1914), and the Corpo Aeronautico Militare of Italy (January 1915) were early independent air services. Kennett, *The First Air War: 1914-1918*: 20.

[97] W. Mitchell and R.S. Ehlers, *Winged Defense: The Development and Possibilities of Modern Air Power--Economic and Military* (University of Alabama Press, 2010), X.

Proposition 1*: In cyber war, offensive cyberpower is the dominant form of cyber warfare.*

Offensive cyber activities ensure superiority in cyberspace while aiding the same in the air and space domains of Air Force operations. By controlling a determined spectrum of cyberspace and preventing the adversary from maneuvering in that cyberspace, a friendly force advantage is created when compared to the adversary. As with any warfare domain, offensive action can be decisive, surprise creates advantage, and freedom to maneuver at a pace quicker than an opponent is desirable. These principles apply to cyber just as they do in air, land, or sea battle.

Proposition 2: *Offensive cyber-actions also contribute to rapid global strike due to the inherent speed at which cyber operations are conducted.*

The effectiveness of these offensive operations is dependent on accurate intelligence and shaping of the cyberspace before and during operations. Additionally, offensive cyber can affect the command and control of an adversary, as well as impacting the nuclear deterrence capability of an adversary. The affects described may be achieved indirectly by targeting supervisory control and data acquisition (SCADA) vulnerabilities and software vulnerabilities, or directly by active hacking into systems for real-time control, activating logic bombs to enable desired effects, or social engineering by making an adversary believe friendly forces are conducting authorized and legitimate activities.

Proposition 3: *The offensive, mass, surprise, maneuver, unity of effort, legitimacy, and proportionality principles of war are most prevalent in offensive cyber operations*

Although all principles of war defined in joint publication or Air Force doctrine will apply to offensive cyber operations at some point, the principles most prevalent are: offensive, mass, surprise, maneuver, unity of effort, legitimacy, and proportionality—proportionality replaces the restraint principle defined by the Air Force.

Proposition 4: *Offensive cyber operations impact all phases of war, but may be most effective in earlier phases for shaping and initial action.*

As for which phases of war offensive actions can and should occur, the author argues it impacts all of them. However, the focus of offensive cyber action should be in phase-0 and phase-1 in order to shape the environment by conducting operations to deter an adversary from escalating to war. Then, if war starts, full scale offensive cyber operations should occur in phase-2 and phase-3 to gain and maintain control of not only cyberspace, but initiate actions that inhibit air, land, and sea operations of an adversary where possible through cyberspace. Finally, offensive cyber actions can assist phase-4 stabilization efforts by countering adversary actions that oppose friendly political objectives. These may include information operation campaigns that support legitimate actions of those suing for peace while inhibiting access in cyberspace for those who oppose peaceful negotiations.

Proposition 5: *Defensive cyber operations are futile if not focused and will not conclude a war. Nations should not attempt to defend all of cyberspace.*
Defensive cyber operations support phase-0, 1, 2, & 4 military operations primarily, although there is a standing requirement for on-going defensive cyber measures both in peacetime and in war. There will always be a need for passive and active defensive measures to protect US national security interests supported by, or potentially affected through, cyberspace. However, defensive cyber operations are not decisive in nature and will not resolve conflicts in cyberspace nor conclude war of any form.

Proposition 6: *Defensive cyber-operations are most relevant when automated response actions occur based on active sensors.*
Relative to the defined Air Force cyber-target roles, defensive cyber operations primarily support air, space, and cyberspace superiority measures through passive and active cyberspace defense mechanisms. Using sensors to detect and report network system anomalies would be one such measure. The overused pursuit of "software patching" on open government systems would be another.[98] The fallacy with the software patching is that its actions are mostly reactive to identified vulnerabilities. For this reason, automated responses must be developed to protect cyberspace relative to national security interests. If human interaction is required to reduce the vulnerability, the time required

[98] Software patching is a software fix distributed by a manufacturer, like Microsoft, to close a known vulnerability. Some software vendors will not support customer needs if software patch updates are not applied and up to date. This process requires the end-user to constantly monitor for software updates. This is a reactive process that requires manual intervention by users. A 2004 survey of US electrical operators found "loosely controlled system access and perimeter control, poor patch and configuration management, and poor system security documentation." Another study found certain systems took an average of 331 days to implement software patch updates. That means vulnerabilities remained for almost an entire year before being corrected. Imagine flying an airplane with a known cracked wing for 331 days. Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*: 98.

for any such action will be an inhibitor due to the speed at which actions occur in cyberspace. Whatever useful method for cyberspace defense is employed, these roles must also support offensive objectives while protecting critical national security targets from adversarial affects.

Proposition 7: *Defensive cyber-forces can rapidly transition to offensive roles thus providing a reserve cyber force for commanders.*

These defensive tactics cannot achieve political objectives in and of themselves; however, if needed, the defense forces can rapidly transition to offensive forces to provide either a counter-attack against an adversary's offensive attack or provide a reserve force if additional offensive forces are needed to exploit a cyberspace gap. Defensive cyber operations can also protect intelligence, surveillance, and reconnaissance, command and control, and nuclear deterrence functions. Operations in these realms are relegated to protecting the information relied upon within these mission sets, while potentially conducting disinformation campaigns through deception techniques such as "honeypots."[99] By conducting these operations, cyber-forces can learn adversary techniques which assist further development of offensive cyber-forces and operational techniques.

Proposition 8: *Economy of force, simplicity, security, and perseverance are the primary principles of war used in conducting defensive cyber operations.*

Because cyberspace is a constantly changing domain, and the adversary is capable of thinking and adjusting to counter new techniques and technology, attempting to defend the entire cyberspace domain is fruitless. Some might argue China is competing with the US by creating havoc in cyberspace thus pushing the US to counter-threats by all necessary means short of kinetic warfare. If that is a battle the US intends to fight, it could potentially be more expensive in the long-run than the Cold War with Russia.[100] As Cold War military capabilities were developed and established, maintenance and readiness of the force were the only recurring costs. Although the costs of cyber

[99] Honeypot is a computer, usually virtual, without any security safeguards, in other words, designed to be infected by malware. Bowden, *Worm: The First Digital World War*: 248.

[100] The average annual cost to the United States military during the Cold War years are estimated at $298.5 billion. The cost of protecting, maintaining, and repairing damages caused by cyber-attacks is unknown today, but should be tracked more accurately to truly assess costs of cyberspace to the nation. See Martin Calhoun, "Center for Defense Information: US Military Spending, 1945-1991, http://academic.brooklyn.cuny.edu/history/johnson/milspend.htm.

technology are extremely cheap to create and maintain relative to a nuclear arsenal, the damage caused by one offensive cyber-attack can potentially be extreme.[101] The challenge with supporting such a claim today is, many organizations who have suffered a cyber-attack may not report it, therefore the actual cost of damage or monetary equivalent in lost information or assets is incomputable.

Proposition 9: *Closed networks are the best protection from an adversary's cyber operations.*

Employing the right size force to provide cyber-security of true national security interests will limit what cyber-forces must protect. This keeps the defensive measures focused and simple. It does not mean cyber-defense techniques are simple verses complex; defense in depth is an absolute must. Persevering through varying cyber-attacks ensures the survivability of required national capabilities so they are available when called to action by policy-makers. Of course, one of the best defenses in the cyberspace battle is to separate critical networks from the less critical; in other words employing a closed network for critical capabilities versus an open network.

The battle for open versus closed networks has already begun. Could it be the authoritarian governments have recognized how vulnerable all warfighting domains are given the pervasiveness of cyberspace and are taking the first steps to minimize risks? In an attempt to institute governmental controls upon the open Internet, 89 countries voted in favor of allowing each nation the authority to close off access to the Internet in their countries.[102] Although 55 of the 193 nations voted against the International Telecommunications Union proposal, the treaty is set to take effect in 2015 without binding its rules to those nations who opposed it. However, even though nations who

[101] According to the "Second Annual Cost of Cyber Crime Study," which is based on a sample size of 50 "larger-sized organizations," the cost of cyber-crime has gone from an average $3.8 million per company to $5.9 million per company for one year. That represents an increase of 56% in one year. Obviously this example may not correlate directly to cyber threats to national security, but based on the importance of centers of gravity discussed in chapter 4, it is safe to presume that cyber-attacks and threats to national security interests are at minimum comparable to these corporations. The bottom line is, if damage from cyber-attacks continues to increase at a rate of 56% per year, defense spending to protect national security interests enabled by cyberspace must keep pace with these threats or succumb to adversarial effects. See Ponemon Institute, "Second Annual Cost of Cyber Crime Study," Benchmark Study of US Companies, August 2011, http://www.hpenterprisesecurity.com/collateral/report/2011_Cost_of_Cyber_Crime_Study_August.pdf.

[102] Gordon Crovitz, "America's First Big Digital Defeat," *The Wall Street Journal,* 16 December 16 2012, http://online.wsj.com/article/SB10001424127887323981504578181533577508260 html.

opposed the treaty are not bound to it, they will be affected by its actions. The global network will be split into two camps—open networks, and closed.[103] This does not change the required offensive, defensive, and exploitation actions in cyberspace, but it may require a change in the tools and techniques to successfully accomplish them.

Proposition 10: *Exploitation in cyberspace is intelligence gathering and will always endure in cyberspace operations and continue throughout all phases of war.* Exploitation is the final capability to connect to defined roles, military phases of and principles of war. Air Force exploitations in cyberspace will be shaped by defined policies recommended previously. Once policy is established surrounding cyberspace operations, and defines what constitutes acts of aggression or acts of war, those conducting acts of exploitation in cyberspace may be more constrained than they are today. Regardless, it is proposed that exploitation actions do and will continue to occur in five of the six defined Air Force roles: air, space, and cyberspace superiority; intelligence, surveillance, and reconnaissance; global strike; command and control; and nuclear deterrence.

These exploitation actions are both against friendly forces to test system resiliency—in the form of red teams—and in the form of intelligence gathering against potential or known adversaries.[104] Exploitation will create the greatest effects during phase-0, 1, & 5 of military operations; however, just as offensive and defensive efforts will cross the full spectrum of military operations, so too will exploitation. Using cyberspace to create vulnerabilities found during exploitation are accomplished with greater autonomy when uncontested; for that reason the three phases of military operation

[103] Given the fact the Internet was designed to be a place for freedom of information interchange without regulation or governance, the creation of closed portions of the Internet my hinder operations in cyberspace. But in reality, this is nothing new. Companies have used closed systems since the Internet's creation; the difference is they have also paid for closed circuits to support the closed systems. This proposal allows for "control over Internet companies, not just telecoms" through its declaration that "all governments should have an equal role and responsibility for international Internet governance." The fallacy in this thought process is, not all governments equally provide the Internet and the realists would argue those with the most power should get the biggest voice. Gordon Crovitz, "America's First Big Digital Defeat," *The Wall Street Journal,* 16 December 2012, http://online.wsj.com/article/SB10001424127887323981504578181533577508260 html.

[104] Red teaming is considered by some to be the "most effective tool we have for testing the security of an information system." In simple terms it is an organization established to probe an organization for security vulnerabilities either through hardware or software misconfiguration or established processes for interacting in, through, or from cyberspace. Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*: 222.

recognized may presumably be the less contested in that they occur before active war begins or immediately at the conclusion of warfare.

To gain the most effort from cyberspace exploits, unity of command, defined targeting objects to exploit, economy of force, and perseverance are necessary principles of war. Given the efforts of exploitation, there is a required collaboration across the varying US civilian and governmental agencies today. Without effective collaboration, there will inevitably be cyberspace fratricide whereas exploitations may overlap a target because multiple agencies are targeting the same objective, or multiple cyber exploit tools are used on the same objective ultimately causing unneeded waste of valuable capabilities. Of the many challenges to generate effective cyberspace exploitation operations, researching and developing effective tools may be the most relentless requirements. Unlike other domains where technology aids in developing long-term fifth generation stealth fighter, new stealth submarine, or high-speed armored personnel carrier, the technology for cyber exploits, as well as some offensive tools, can expect to have a relatively short shelf-life and may be good for only one use. These are facts driven by the dynamic nature of cyberspace and its constantly changing character.

Despite the challenges to exploitation efforts, and the fact that it exists to aid both offensive and defensive cyber operations, as well as all other warfighting domains, its value cannot be understated. In future wars where it may not be nation-state versus nation-state, the more information regarding cyberspace vulnerabilities and developing exploits that will have known effects, the more prepared US forces will be for the next war. Preparing for war requires having known capabilities to present to combatant commanders during planning and execution in order to bring about decisive victory in war. If a commander employs cyber-capabilities that create a loss of confidence in the adversary's command and control before battle begins, one can only imagine the true fog and friction that will occur if that adversary presses for war. Compound that confusion with others that will result in an all-out cyber offensive upon determined centers of gravity, while synchronized with other warfighting capabilities across all domains, and overwhelming the enemy is clearly the principle objective for rapid capitulation in war.

Anticipate

Figuring out how and when to employ the offensive, defensive, and exploitation capabilities in cyberspace is a constant challenge for military forces today. This is especially true in an environment of unresolved legal concerns surrounding actions in cyberspace, undefined policy regarding acceptable and unacceptable cyberspace behaviors, and the gray area surrounding potential reactions to cyber-threats given the challenges of attribution. However, these concerns do not justify inaction in planning, developing, and validating cyber capabilities. The US National Security Strategy calls for protection of its citizen's security, prosperity, values, and international order. The author argues cyberspace is eroding each of these stated interests within the US borders and internationally every day. The rules regarding stealing of intellectual property and US secrets which compromise the technical advantages the US is known for are undefined in international law and not yet classified as illegal activity in cyberspace; at least not for all nations.[105] If left unchanged, nations will continue to lose trust both domestically and internationally as actors within cyberspace conduct acts of crime, terrorism, and espionage. How long can the US afford to not step out and take a lead role in establishing standards and acceptable behaviors throughout cyberspace?

Despite these challenges, many steps are being taken to counter known threats and prepare for future warfare which will include cyber war. Lawyers are pouring through laws of armed conflict, international laws, and domestic laws at an unprecedented rate to determine what if any changes need to be made.[106] There is little doubt some laws will change, presumably in the area of identifying and responding to initial cyber-threats. It should not matter what virtual force, whether civilian or varying military, respond to stop an initial cyber-threat, as long as the threat is mitigated. To

[105] Part of the challenge in defining international rules surround the lack of common terminology for cyber related activities. Accepting common definitions for terminology such as cybercrime, cyberterrorism, and cyberwarfare is one start to developing international standards. Susan Brenner offers a common lexicon to consider. Once the lexicon is agreed upon, then international standards of behavior within cyberspace may begin to evolve. Brenner, *Cyberthreats: The Emerging Fault Lines of the Nation State*: 29-54.

[106] For a detailed three year research regarding international laws surrounding cyberwar, see the work of twenty international law scholars and practitioners. This work lays out ninety-five rules governing cyber warfare. The rules range from actions before cyber war to conduct in war, as well as international humanitarian law and laws of neutrality. M.N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, 2013).

achieve these results, at least domestically, the delineation between guard, active duty forces, or some other national, state, or local law enforcement agency tasked to respond with a physical presence must become seamless in order to respond to cyber-threats.[107]

Technologies continue to improve and will eventually resolve the perceived attribution challenge within cyberspace. This challenge is already much less than it was just a couple of years ago because forensic testing is getting better both in technology and by virtue of doing more of it. As with anything, the more something is done the more we humans tend to get better at doing it. This leads to the continual advancement of education and training in all areas of cyber. As threats like denial of service emerge as major threats to operational success, education and training increase along with technology to counter these threats. The intent should not be to eliminate these types of threats as that is most likely unrealistic; however, controlling and containing them so they do not prevent mission success is absolutely a realistic and attainable objective.

As the US society continues to see the vulnerabilities of cyberspace and the ripple effect in damage that can be caused, mostly in replacement costs of technical capabilities and loss of consumer confidence, pursuit of government involvement to control cyberspace threats will grow. In the commercial industry, for activities that do not directly threaten the society as a whole or its national security interests, those challenges will provide capitalistic opportunities for problem resolution. For cyberspace threats that challenge sovereignty, a society's cultural beliefs, and its security, government oversight will occur. When this call for government intervention occurs, the loss of anonymity which some pundits argue as the nemesis to greater cyber-security now will become voices of the past. These same evolutions have occurred since the beginning of time and will continue to occur as societies progress no matter what new technologies evolve, or how much freedoms societies pursue.[108] As long as man's nature remains unchanged—

[107] Within the domestic realm, US military forces operating under Title 10 authorities are prohibited from conducting military operations without special provision. The 1878 Posse Comitatus Act created a distinction between military and civilian law enforcement within the US. It is laws such as these that require consideration in order to resolve response actions to cyber-threats. Brenner, *Cyberthreats: The Emerging Fault Lines of the Nation State*: 177.

[108] Susan Brenner discusses how by the mid-twentieth century, nation-states monopolized the legitimate use of force to maintain order, both internally and externally. They relied on professional, uniformed, hierarchically organized warriors to resolve external conflicts arising with other nation-states; and they relied on professionals, uniformed, hierarchically organized law enforcement officers to maintain internal order by reacting to the commission of crimes within the territory the nation-state controlled. This is the

principle concern is survival—there will be a need to create order in the anarchic world in which man lives.[109]

Testing

If the object of science is knowledge and the object of art is creative ability, the theory proposed regarding offensive, defensive, and exploitation of cyberspace is art.[110] By defining specific cyber targets to help shape organize, train, and equip endeavors for Air Force cyber-forces, and presumably all US military forces, as well as national objectives involving cyberspace, the appearance of a scientific way for cyberwar appears prevalent. However, this is a fallacy. Without experience, facts, or tested theories, a normal science of cyberwar does not exist; at least not until it has been tested.[111] This is the very reason this author believes testing is required for this theory's development. Without testing or experience to rely upon, is an untested theory just a hypothesis?[112]

Efforts to test cyber capabilities are well underway, as are efforts to include cyberspace operations into existing Air Force functions. Air Combat Command is currently updating a targeting roadmap which intends to incorporate cyber-targets into

same premise which should be considered to control cyber-crimes as it has and continues to work for other protection of the nation-state and its citizens. Brenner, *Cyberthreats: The Emerging Fault Lines of the Nation State*: 23.

[109] Kenneth Waltz claims there is no automatic harmony in anarchy. Waltz is referring to the order of the international system and relation between states as he describes the world order as a system of anarchy. He states that with no system of law enforceable among sovereign states, each state will judge its grievances and ambitions according to the dictates of its own reason or desire—conflict, sometimes leads to war. Concerns regarding international order of acceptable norms within cyberspace exist in this same system of anarchy that is the international system today. Waltz*, Man, the State, and War: A Theoretical Analysis*: 160.

[110] Clausewitz, *On War*,149.

[111] In discussing normal science, Thomas Kuhn states science is the constellation of facts, theories, and methods collected in texts. It is these accepted scientific proofs which create the "normal science" environment. Thomas Kuhn, *The Structure of Scientific Revolution*, 1.

[112] There is a difference in a scientific hypothesis—untested but proposed explanation—versus a scientific theory—extensive testing is conducted and generally accepted as an accurate explanation. Richard Rumelt defines a scientific hypothesis as "a new idea or theory," but this type of definition muddies the discussion as a hypothesis and theory are not exactly synonymous (although dictionaries do show them as synonyms.) R. Rumelt, *Good Strategy Bad Strategy: The Difference and Why It Matters* (Crown Publishing Group, 2011), 247. The author's interpretation is that a hypothesis is "a tentative assumption" before testing, where as a theory is a "plausible or scientifically acceptable general principle or body of principles offered to explain phenomena." In other words, a hypothesis is untested, and a theory has parameters to test against that are already accepted as norms. *Merriam-Webster's Collegiate Dictionary: Eleventh Edition*, (Merriam-Webster, Incorporated, 2004).

the current Air Force targeting cycle.[113] This includes building targeting folders, collecting intelligence, and at least having applicable discussions of where cyber fits into the current Air Force targeting doctrine. But does this process allow cyber to conduct its full spectrum capabilities? Are the targeting objectives based on effects enabled by cyberpower and offensive tools available to a combatant commander, or is cyber relegated to a support role with airpower capabilities at the center of offensive planning efforts? These questions are beyond this treatise, but are worth future debate. Just as airpower and its relevance as an independent fighting force was worth having in the early 1900's, so too should cyberpower's unbounded capabilities be explored to determine its role as a military power and its ability to achieve political objectives. Regardless of the outcome, by including cyber discussions and potentially testing capabilities, the proposed cyberpower targeting theory can move toward a true theory as continual experience is gained.

Other efforts to test cyberpower abilities expand continually in joint cyber-exercises.[114] Over the past few years the cyber injects have gone from white-card notional applications of cyberpower to true operational testing of cyber capabilities. The lessons learned from second and third order cyber-effects in the exercise scenarios certainly aid continual improvements. Expansion in military cyber-ranges enable integrated training and education not only within the Air Force, but with sister services and civilian agencies alike.[115] These low cost resources pay huge benefits by bringing

[113] The purpose of the Air Force Targeting Roadmap is to, "The Air Force Targeting Roadmap provides the foundation to develop an action plan to revitalize Air Force targeting capability and ensure that the Air Force is organized, trained and equipped to support Joint and Coalition Forces. This roadmap articulates Air Force senior leaders' guidance to drive policy and resource decisions that achieve a robust, effective, and efficient Air Force targeting capability." For more specifics, see "Air Force Targeting Roadmap: Reinvigorating Air Force Targeting," 30 September 2012, 8.

[114] The joint cyber forces train together in cyber ranges intended to validate "cyber technologies by emulating complex defense and commercial networks." See *Air Force Magazine*, "National Cyber Range Completes Beta Phase," 21 November 2012. Additionally, joint exercises that go beyond the virtual cyber ranges include activities such as Terminal Fury 2011. Exercises such as these enable operational testing of concepts like Adaptive Network Defense of Command and Control which enables joint force commander control of key terrain in cyberspace. These are exactly the synchronized efforts cyber-forces will require to confront the adaptive nature cyberspace affords adversaries who will choose to confront the US in the newest warfighting domain. For more on Terminal Fury, see: Major Jose Gonzalez, "Joint Experimentation Enables Regional Cyber Protection," *Signal,* 1 February 2013.

[115] There is already movement toward joint cyber training centers of excellence. The CyberCity is one such example. The operation, which is run by a New Jersey-based security firm is intended to provide soldier-hackers from the Air Force and other branches of the military with practice in attacking and defending computers and networks that run a theoretical town. Robert O'Harrow Jr., *The Washington Post,*

disparate cyber operators to a common understanding of the contested cyberspace environment. This also allows for real-time sharing of cyber tools and techniques that improve cyber-security practices, while testing new capabilities off the "live network."[116]

Testing this theory requires more than just validating technological capabilities of cyberspace tools. Cyberspace relies on human capital to create affects in the cyber domain. One could argue this is true for all domains, but it is especially true in cyberspace. Without human capital the cyberspace domain has no need to exist or function since its purpose is to serve societal needs. This is not true for the other domains. Land, air, sea, and space would all continue to exist without human intervention. Together these global commons constitute the connective tissue of the international system affecting various aspects of societies.[117]

Given this reliance of the cyberspace domain on the human, it is important to continually test the on-going education, training, and experiences of human development regarding cyber-forces. If US military forces are going to dominate in cyberspace, capital investments in higher education, state-of-the-art training centers, and operational experience are critical to success. Once this occurs, the cultural development needed for consistent cyber activities can be facilitated.[118] But US forces must be cautious in the pursuit to make the perfect cyber-operator.

Despite theories such as cybernetics and chaoplexity espoused by Antoine Bousquet which pursue both the human drive for complete predictability and the desire for control in warfare, those should not be the human pursuit in regards to cyberwar.[119] Historical examples continually remind us that the pursuit of complete predictability is unattainable; however, there are actions that can reduce some fog and friction in war.

"CyberCity allows government hackers to train for attacks," 26 November 2012, http://articles.washingtonpost.com/2012-11-26/news/35508198_1_government-hackers-security-firm-digital-attacks.

[116] Live network is sometimes the name given to the open Internet. If a training exercise goes bad, the effects are not felt by users of the public. These cyber-ranges can be viewed as virtual simulator training like pilots use for training. This way if a plane crashes during simulator training, there is no physical damage or real-world costs.

[117] See The Quadrennial Review in Betz and Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-power*: 8.

[118] Stuart Starr, "Toward a Preliminary Theory of Cyberpower," Kramer, Starr, and Wentz, *Cyberpower and National Security*: 48.

[119] See cybernetic warfare and computers, and chaoplexic warfare and the network in Bousquet, *The Scientific Way of Warfare: Order and Chaos on the Battle Fields of Modernity*: 33-34.

Efforts such as incorporating cyber-warriors into existing weapons instructor courses are a great first step.[120] Not only does this program provide an opportunity for other Combat Air Force platforms to understand what cyberpower can do, it exposes cyber-operators to other combat platforms. The result is greater understanding of existing capabilities and potentially better integration of combat efforts.

Another positive movement by the Air Force is professing the need to stand up a Cyber Air Corps Tactical School (C-ACTS) in order to expand strategic thinking regarding cyber capabilities while evolving doctrine on the subject.[121] Efforts like this develop the human aspect by discussing the art-of-the-possible relative to cyberpower projection, while creating an environment to analyze academic rigor and determine required adjustments to continually develop the force and the cyberpower strategies to be used by the force. Although these early discussions may not provide the best possible results in the first cyber war, they will provide a foundation for future discussions as knowledge is gained, feedback is received, and new challenges arise.

The final piece of testing discussed in this treatise revolves around obtaining lessons learned in operations and applicable metrics for measuring intended cyber results. This may be one of the most challenging objectives, to develop meaningful battle damage assessment of cyberpower effects. Although cyberpower has the ability to be extremely precise in its targeted effects, it also has the potential to create massive unintended second and third-order effects if fail-safes are not embedded correctly. Stuxnet may be a great case study to make this point. It has been argued Stuxnet was created with a specific target in mind. However, when the Stuxnet exploit crossed over from a closed

[120] The Twenty-Fourth Air Force developed a "Weapons and Tactics Roadmap" in 2011 to help shape the development of an operational cyber force in regards to cyber warfare. Although the roadmap has not been approved/signed as of this writing, the Air Force has already moved forward with developing its cyber warriors. 2012 marked the first cyber weapons school class which developed both cadre and field tacticians alike. In addition to education and training, the Air Force cyber community has also developed a tiered list for outplacement of these highly skilled Airmen which affords development and experience opportunities from the tactical through strategic levels. This effort is a great start in developing a required cadre of experts the Air Force must invest in for its future success in cyber-war. See the unpublished draft of the Air Force Space Command, "Twenty-Fourth Air Force Weapons and Tactics Roadmap," 2011.

[121] Advocacy to gather critical strategic thinkers from all the key players in government and the private sector for the purpose of advancing thought in the new domain of cyberspace recently occurred in a recent Air & Space Power Journal. The authors proclaimed that standing up a "cyber" ACTS, similar to the Air Corps Tactical School for airpower during its infancy, would leverage talent resources from academia, research and development, and operational experience to cultivate ideas regarding cyberspace. To read the full article, see: Lieutenant General David Fadok and Dr. Richard Raines, "Driving towards Success in the Air Force Cyber Mission," *Air & Space Power Journal*, (September-October 2012).

network to an open one, it had the potential to create unintended havoc. Gathering feedback from events such as Stuxnet can aid offensive, defensive, and exploitation operatives develop effective tools and preventative mechanisms as applicable. This will help minimize unintended collateral damage while operating within tolerable risk parameters. The challenge is how are these successes or failures measured, and measured quickly so the information is timely and useful? Once again, this is a question for future study, but one of relevant importance.

Summary

Early skeptics of airpower stated airpower can "hold nothing."[122] Recognizing that fact did not constrain the thinking of airpower advocates who sought to expand military capabilities within the newest warfare domain at the time. The same skeptics stated airpower could not hold its ground and fight; this proved to be incorrect in the sense that if a nation was willing they could expend the necessary resources to establish and hold air supremacy. The same can be said in regards to cyberpower today.

Conducting operations in, through, and from cyberspace requires unbounded evaluation of the art-of-possible while recognizing the limitations inherent to the nature of cyber operations. Cyber operations will never hold the physical ground that ground commanders refer to. This author suggests that holding ground is not a requirement of cyber operations; nor should it be—at least not until the ground force is robotic, at which point cyber forces can hold the ground. As long as US national security is protected from harmful cyber-attacks, and effective US cyber operations are enabled to meet political objectives, then the efficacy desired is achieved.

Cyberspace is changing most rapidly among warfighting domains, driven by the fact it is the only man-made domain where warfare can occur. Recognizing this fact, despite the minimal expense of operating in cyberspace, highlights the fact that 'holding' permanently the cyberspace ground is unattainable. However, controlling a portion of the cyberspace domain, while conducting required operations, is quite probable. Protecting US vital interests from cyberspace threats requires the Air Force and other services to not

[122] Sherry, *The Rise of American Air Power: The Creation of Armageddon*: 63.

only employ cyberpower within this warfighting domain, but dominate portions of it to ensure operational success is achieved across all warfighting domains.

Just as nations build airplanes to dominate air, ships to dominate sea, and armies to dominate land, so too must nations build cyber technology and develop cyber warriors to dominate cyberspace. If the cyberpower targeting theory espoused aids in continual doctrine development, strategic thinking regarding the possibilities of cyberpower, and is considered during organize, train, and equip decisions for cyber-forces in the USAF and potentially national level, then the intent of this treatise is achieved.

Given the lack of cyber war and cyber warfare experience, limited definitions regarding what constitutes cyber war, and minimal publishing's of cyber war doctrine, maybe the best this thesis can suggest is a 'hypothetical theory for strategic cyberpower.' Based on the author's understanding of Clausewitz, familiarity with a theory requires analytical investigation with the subject and applied experience—relative to military history in this case—to gain thorough familiarity with it.[123] Theory then becomes a guide to anyone who wants to learn about war in books, preventing warriors from starting warfare studies afresh each time war occurs.[124] Either way, the fact that cyberpower is being discussed, and theories of cyber war are evolving, this author is confident the US military will continue to develop cyber-warfare capabilities and enable independent, as well as integrated cyberspace operations in order to win the nation's future wars.

[123] Clausewitz, Howard, and Paret, *On War*: 141.
[124] Clausewitz, Howard, and Paret, *On War*: 141.

Chapter 6

Conclusion

> *The acceptance or rejection of an invention, or to the extent to which its implications are realized if it is accepted, depends quite as much upon the condition of society, and upon the imagination of its leaders, as upon the nature of the technological item itself.*
>
> Lynn White

Major General Suzanne Vautrinot, commander of Air Force cyber forces, argues that the Air Force can leverage cyberspace to create integrated effects to respond to crisis and conduct uninterrupted operations.[1] This author agrees, but recommends the Air Force define clearly what cyberspace effects it desires to create so that the Air Force is organizing, training, and equipping a cyber-force ready to respond to tomorrow's crisis. By publicly announcing that Air Force policy is to defend specific national security interests, as well as, actively oppose cyber-attacks with offensive cyber-operations, cyberspace security surrounding military operations will increase while cyber-force professionals gain invaluable experience. By defining acceptable and unacceptable behaviors, and publicizing them, international norms will no longer be left to arbitrary precedence. These actions will drive cyberspace standards within the US military; as well as acceptable US and international norms throughout cyberspace. If the US chooses not to lead cyber-security efforts, another nation will and it may not be in the direction of US national interests. If this occurs, US cyberspace operations will become more reactive than they are currently today.

Evaluating the early theories of airpower advocates like Douhet, Trenchard, and Mitchell can aid cyber-theorists today. By understanding and identifying where cyberpower can influence military operations and target adversary centers of gravity will shape US military efforts in achieving political objectives. However, given the infancy of cyberspace, along with the limited use of cyberpower to influence conflict resolution, many military cyberspace operations are guided by hypothetical potential versus tested results. It is applicable for the US Air Force to examine the theory and doctrine, as well as the tactics, techniques, and procedures the Air Corps Tactical School (ACTS)

[1] Major General Suzanne Vautrinot, "Sharing the Cyber Journey," *Strategic Studies Quarterly* 6, no. 3, (Fall 2012): 80.

evaluated throughout the 1920s and 1930s. Airpower targeting theories such as the Industrial Web Theory guided Army Air Corps education and training objectives before World War II; it also shaped the organize, train, and equip functions by focusing airpower efforts through the use of a combined bomber offensive. Although these early theories are controversial to some, the reality is, advocates focused on desired results and continued to learn through the use of airpower what worked well and what did not. Continual evolution of technology eventually led airpower to become the force multiplier early advocates perceived it could be.

It can be argued Operation DESERT STORM was airpower's defining moment. The technology of airpower evolved to a point that precision bombing became a reality and the speed and agility of which airpower could strike was realized. Combine the system capabilities of airpower with the contemporary airpower theory of Colonel John Warden, and airpower destroyed effectively the enemy's ability to operate as an effective fighting force. Cyberpower theorists today can draw upon the doctrine, education, and training focus of the ACTS and combine them with the strategic perspective of viewing the enemy as a system that Colonel Warden suggests, to develop an effective cyberpower targeting theory for use in future conflicts. There is little doubt that cyberspace will be employed before, during, and after all future wars; in shaping the battleground, initiating a conflict, or throughout all phases of military operations.

As military commanders evaluate the offensive, defensive, and exploitation roles cyberspace affords, there are limitations today which prevent a military's use of cyberspace from reaching its full potential. Attribution, authorities, and understanding centers of gravity which can be targeted by cyberpower are but a few of the challenges to wielding cyberpower. As civilian and military leaders grapple with these challenges a review of the required expertise and organization necessary to support cyberspace efforts may be required. As the US seeks to protect its national security interests in, through, and from cyberspace activities, accepting cyberspace as a distinct domain has significant implications for equipping cyber-forces and developing a culture for cyber activities.[2] These discussions may sound familiar to early airpower supporters who advocated a separate service before 1947 and thus are worth discussion in the fiscally strained

[2] Kramer, Starr, and Wentz, *Cyberpower and National Security*: 48.

environments of today, especially if duplication and inefficiencies are found across each service's efforts to wield cyberpower.

Cyberpower has not changed the nature of war; however, it has changed the character. Military forces who want to be successful at winning future conflicts must embrace the potential affects and effects wielded by cyberpower. Commanders must organize, train, and equip cyber-forces to achieve desired results while limiting the impacts of the adversary from doing the same to friendly and allied force actions. Given the minimal lessons of cyber-warfare that exists today, theorizing about cyberpower effects and their cause is relevant today. Although early theories may not lead to doctrinal principles that last through time, they will be an attempt at understanding the potential of cyberpower. The choice to employ offense, defense, or exploitation as the primary role of US cyberpower should not be arbitrary; something that appears to be the case across the international community today. If the US defines what constitutes cyber war and cyber warfare, then defines acceptable and unacceptable behaviors, the US will begin to shape international norms throughout cyberspace. It seems prudent for the US to shape these efforts today vice allow the international community to dictate norms that does not protect US national security interests.

This author's intent is to espouse a cyberpower targeting theory, along with initial propositions of cyberpower, to continue the dialog regarding US cyberpower. Learning lessons from the evolution of airpower may not only shape how US military forces employ cyberpower tomorrow, but also save the nation's treasure by preventing similar mistakes of the past. If critical thinking surrounding cyberspace efforts enhance organize, train, and equip endeavors of military forces, then militaries and policy-makers alike are serving national interests accordingly. Finally, by thinking about the true potential of cyberpower, American vulnerabilities to adversary actions in, through, or from cyberspace should become evident. When this occurs, gaps can be closed and confidence in future cyberspace operations and security should increase. Given the current and continued reliance on cyberspace by societies, especially the US society, the vulnerabilities of democracies like the US to cyber-attack are real. Therefore, it is critical the US continually evaluate cyberpower both of the US and her allies, and those of potential adversaries, if the nation truly intends to protect its national interests.

Bibliography

Air Combat Command, “Air Force Targeting Roadmap: Reinvigorating Air Force Targeting,” 30 September 2012, 8.

Air Force Doctrine Document (AFDD) 1, *Air Force Basic Doctrine, Organization, and Command*,14 October 2011.

Air Force Doctrine Document (AFDD) 3-12, *Cyberspace Operations*, Change 1, 30 November 2011.

Air Force Doctrine Document (AFDD) 3-60*, Targeting*, Change 1, 28 July 2011.

Air Force Instruction, 14-117, I*ntelligence: Air Force Targeting,* 13 May 2009, 1.5, 6.

Air War Plans Division, Plan – 1, “The Process.” http://www.au.af.mil/au/awc/awcgate/readings/awpd-1-jfacc/awpdproc.htm.

Air War Plans Division (AWPD) - 42, pt. 4, “Report,” AFHRA, 145.82–42, 2.

Air War Plans Division (AWPD) - 42, tab B-1-a, “Air Offensive—Europe,” Air Force Historical Research Agency, 145.82–42.

Amoroso, E. *Cyber Attacks: Protecting National Infrastructure*: Elsevier Science, 2010.

Anderson, Major General Orville, *Air University Quarterly Review*, “Air Warfare and Morality, 2 (winter 1949): 7.

Arnold, General Henry, Memorandum to the Chief of Staff, Subject: Combat Aircraft Which Should Be Produced in the United States in 1943, 9 September 1942, pt. 2; and “Answering Memo and Outline of Report,” in AWPD-42, AFHRA, 145.82–42.

Belote, Major Howard, “Warden and the Air Corps Tactical School: What Goes Around Comes Around,” *Airpower Journal*, (Fall 1999).

Betz, D.J., and T. Stevens. *Cyberspace and the State: Toward a Strategy for Cyberpower*: Taylor & Francis Group, 2012.

Biddle, T.D. *Rhetoric and Reality in Air Warfare: The Evolution of British and American Ideas About Strategic Bombing, 1914-1945*: Princeton University Press, 2004.

Bousquet, A. *The Scientific Way of Warfare: Order and Chaos on the Battle Fields of Modernity*: Columbia University Press, 2010.

Bowden, M. *Worm: The First Digital World War*: Grove/Atlantic, 2011.

Boyd, Colonel (r) John, Compendium, “The Essence of Winning and Losing,” August 2010. http://dnipogo.org/?s=essence+of+winning+and+losing.

Brenner, J. *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*: Penguin Press, 2011.

Brenner, S.W. *Cyberthreats: The Emerging Fault Lines of the Nation State*: Oxford University Press, 2009.

Brodie, B. *Strategy in the Missile Age: Theory and Applications*: National Book Network, 2007.

Bumgarner, John, “Computers as Weapons of War,” *IO Journal* (May 2010). http://www.nxtbook.com/nxtbooks/naylor/JEDQ0210/index.php?startid=4#/4.

Calhoun, Martin, “US Military Spending, 1945-1991, *Center for Defense Information*.” http://academic.brooklyn.cuny.edu/history/johnson/milspend.htm.

Carroll, L. *Alice's Adventures in Wonderland*: Mac Millan, 1869.

Clarke, R.A., and R. Knake. *Cyber War: The Next Threat to National Security and What to Do About It*: HarperCollins, 2010.

Center for Global Development, “Phase Zero: The Pentagon’s Latest Big Idea,” 20 July 2007. http://blogs.cgdev.org/globaldevelopment/2007/07/phase-zero-the-pentagons-lates.php.

Clausewitz, Carl von, M.E. Howard, and P. Paret. *On War*: Princeton University Press, 1989.

Clodfelter, M. *The Limits of Airpower: The American Bombing of North Vietnam*: University of Nebraska Press, 2006.

Cody, James R., “AWPD-42 to Instant Thunder,” School of Advanced Airpower Studies, June 1996.

Cox, Cameron, “NSA Director on Cyberattacks: ‘Everybody’s' Getting Hit,” *ABC News Radio*, 7 November 2012, http://abcnewsradioonline.com/business-news/tag/hackers.

Craig, P.C. *Destroying the Village: The Prospect of Thermonuclear War in American Security Policy*: Columbia University Press, 1998.

Crane, C.C. *American Airpower Strategy in Korea, 1950-1953*: University Press of Kansas, 2000.

Defense Technical Information Center, Air University Library, Maxwell Air Force Base, AL., M-U 42992-167 c.1, Iris 317878.

De Seversky, A.P. *Victory through Airpower*: Simon and Schuster, 1942.

Department of the Air Force, “Fiscal Year 2013 Air Force Posture Statement.” http://www.afa.org/PresidentsCorner/WashingtonPerspective/2012/02282012_HASC_USAF_Joint_Statement.pdf.

Department of Defense, *DOD Strategy for Operating in Cyberspace*, July 2011.

Dolman, E.C. *Astropolitik: Classical Geopolitics in the Space Age*: Taylor & Francis, 2001.

Donnelly, John, “Cohen: Attack on US Satellite Is Attack on United States,” *Defense Week*, 26 July 1999.

Douhet, G., J.P. Harahan, R.H. Kohn, and D. Ferrari, *The Command of the Air*: University of Alabama Press, 2009.

Dunlap, Charles, “Perspectives for Cyber Strategists on Law for Cyberwar,” Strategic Studies Quarterly (Spring 2011), 81.

Faber, Lieutenant Colonel Peter, "Competing Theories of Airpower: A Language for Analysis," paper presented at the Aerospace Power Doctrine Symposium, Maxwell AFB, AL., 30 April 1996.

Fadok, Lieutenant General David and Raines, Dr. Richard, “Driving towards Success in the Air Force Cyber Mission,” *Air & Space Power Journal*, (September-October 2012).

Federation of American Scientists, Intelligence Resource Program, “Congress Authorizes Offensive Military Action in Cyberspace in FY2012 Defense Authorization Act,” [Sec. 954, Military Activities in Cyberspace], 12 December 2011, 4.

Ferrill, A. *The Origins of War: From the Stone Age to Alexander the Great*: Westview Press, 1997.

Finney, R.T., and Center for Air Force History. *History of the Air Corps Tactical School, 1920-1940*: Center for Air Force History, 1955.

Fischer, Eric, Congressional Research Service Report for Congress, “Federal Law Relating to Cybersecurity: Discussion of Proposed Revisions,” 9 November 2012. http://www.fas.org/sgp/crs/natsec/R42114.pdf.

Forsyth Jr., Dr. James, “What Great Powers Make It: International Order and the Logic of Cooperation in Cyberspace,” *Strategic Studies Quarterly* 7, no.1, (Spring, 2013).

Foulois, Major General Benjamin, Transcript of oral history interview December 9, 1965, U.S.A.F.H.R.C, Maxwell AFB, p. 43.

Fryer-Biggs, Zachary, *Defense News*, “Panetta Lays Out New Cyber Policy,” 12 October 2012. http://www.defensenews.com/article/20121012/DEFREG02/310120002/.

Futrell, R.F. *Ideas Concepts Doctrine : Basic Thinking in the United States Air Force*: DIANE Publishing, 1971.

Futrell, Robert Frank, *Ideas, Concepts, Doctrine*, vol. 2, "Basic Thinking in the United States Air Force," 1961–1984 (Maxwell AFB, AL: Air University Press, 1989).

Gertz, Bill, Counter Proliferation Center, DC to Beijing: Stand Down on Cyber, 11 March 2013. http://freebeacon.com/d-c-to-beijing-stand-down-on-cyber/.

Gillard, Julia, Prime Minister of Australia, *Press Office*, “Australia’s National Security Beyond the 9/11 Decade, 23 January 2013. http://www.pm.gov.au/press-office/australias-national-security-beyond-911-decade.

Glock, Captain John, “The Evolution of Air Force Targeting,” *Airpower Journal*, Fall 1994.

Goldstein, F.L., and B.F. Findley. *Psychological Operations: Principles and Case Studies*: Air University Press, 1996.

Gonzalez, Jose, “Joint Experimentation Enables Regional Cyber Protection,” *Signal*,1 February 2013.

Gray, C.S., and B.S. Lambeth. *Airpower for Strategic Effect*: Military Studies Press, 2012.

Gray, Colin, The Airpower Advantage in Future Warfare: The Need for Strategy, Air Force Doctrine and Development Education Center, Research paper 2007-2 (December 2007), 12.

Gross, Michael Joseph, ‘A Declaration of Cyber-War’, *Vanity Fair*, April 2011. http://www.vanityfair.com/culture/features/2011/04/stuxnet-201104, 1.

Grossman, D., and L.W. Christensen. *On Combat: The Psychology and Phsiology of Deadly Conflict in War and Peace*: PPCT Research Publications, 2007.

Hadnagy, C., and P. Wilson. *Social Engineering: The Art of Human Hacking*: Wiley, 2010.

Hague Convention of 1907 on the Opening of Hostilities, “Declaration of War.” http://en.wikipedia.org/wiki/Declaration_of_war.

Hallion, R. *Storm over Iraq Pb*: Smithsonian, 1997.

———. *Storm over Iraq: Airpower and the Gulf War*: Smithsonian Institution Press, 1992.

Hansell, H.S. *The Air Plan That Defeated Hitler*: Arno Press, 1980.

Hart, Gary, “After bin Laden: Security Strategy and the Global Commons,” *Survival: Global Politics and Strategy,* (Vol.53 no.4, August-September 2011).

Hicks, W.J. *The Command of the Air*: Nisbet, 1916.

Hoig, S., P. Rosier, and A.E. Deer. *The Cheyenne*: Facts On File, Incorporated, 2009.

Hughes, D. *Moltke on the Art of War: Selected Writings*: Random House Publishing Group, 1995.

Hurley, A.F. *Billy Mitchell, Crusader for Airpower*: Indiana University Press, 1975.

Hurley, Matthew, “For and from Cyberspace: Conceptualizing Cyber Intelligence, Surveillance, and Reconnaissance,” *Air & Space Power Journal*, November-December 2012. http://www.airpower.au.af.mil/digital/pdf/articles/Nov-Dec-2012/F-Hurley.pdf.

Hurwitz, Roger, “Depleted Trust in the Cyber Commons,” *Strategic Studies Quarterly* 6, no.3, (Fall 2012.

Jabbour, Kamal, The Science and Technology of Cyber Operations, *High Frontier* 5, no. 3, (May 2009). http://www.afspc.af.mil/shared/media/document/AFD-090519-102.pdf.

Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms*, 15 March 2013.

Joint Publication 3-0, *Joint Operations,* 11 August 2011.

Joint Publication 3-60, *Joint Targeting*, 13 April 2007.

Joint Publication 5-0, *Joint Operation Planning*, 11 August 2011.

Kainikara, S., and RAAF Airpower Development Centre. *Principles of War and Airpower*: Airpower Development Centre, 2011.

Kalyvas, S.N. *The Logic of Violence in Civil War*: Cambridge University Press, 2006.

Keaney, T.A., E. Cohen, and Gulf War Airpower Survey Review Committee. *Gulf War Airpower Survey, Volume Ii: Operations and Effects and Effectiveness*: United States Dept. of Defense, 1993.

Kennett, L. *The First Air War: 1914-1918*: Simon & Schuster, 1999.

Kramer, F.D., S.H. Starr, and L. Wentz. *Cyberpower and National Security*: Potomac Books Incorporated, 2009.

Krekel, B.A., Northrop Grumman Corporation, P. Adams, G. Bakos, U.S.-China Economic, and Security Review Commission. *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*: CreateSpace Independent Publishing Platform, 2012.

Kuhn, T.S.A. *The Structure of Scientific Revolutions*: University of Chicago Press, 1996.

Libicki, M.C. *Cyberdeterrence and Cyberwar*: RAND Corporation, 2009.

Libicki, Martin, “The Specter of Non-Obvious Warfare,” *Strategic Studies Quarterly* 6, no. 3, (Fall 2012).

Lin, Patrick, Allhoff, Fritz, and Rowe, Neil, *The Atlantic*, “Is It Possible to Wage a Just Cyberwar?”. http://www.theatlantic.com/technology/archive/2012/06/is-it-possible-to-wage-a-just-cyberwar/258106/#.UKJ8Z_mRMQ0.email.

Lonsdale, D.J. *The Nature of War in the Information Age: Clausewitzian Future*: Frank Cass, 2004.

Lun, Xinxi Duikang, *Information Confrontation Theory,* China Publication Library, 2007.

Lynn, William, “The Pentagon’s Cyberstrategy: One Year Later,” *Foreign Affairs*, (28 September 2011)

Maurer, Tim, "Cyber Norm Emergence At the United Nations," (September 2011). http://belfercenter.ksg.harvard.edu/files/maurer-cyber-norm-dp-2011-11-final.pdf.

McDougall, W.A. ...*The Heavens and the Earth: A Political History of the Space Age*: Johns Hopkins University Press, 1997.

Mellinger, Phillip S., "Ten Propositions Regarding Airpower," *Airpower Journal* 7, no. 2, Summer 1993.

Merriam-Webster's Collegiate Dictionary: Eleventh Edition. Merriam-Webster, Incorporated, 2004.

Miller, R.G., and P. R Miller. *To Save a City: The Berlin Airlift, 1948-1949*: Texas A&M University Press, 2008.

Mitchell, W., and R.S. Ehlers. *Winged Defense: The Development and Possibilities of Modern Airpower--Economic and Military*: University of Alabama Press, 2010.

Morgan, F.E., and Project Air Force. *Deterrence and First-Strike Stability in Space: A Preliminary Assessment*: RAND Corporation, 2010.

Momyer, William W., *Airpower in Three Wars*, Washington, D.C.: Department of the Air Force, 1978.

Morrocco, John D., "From Vietnam to Desert Storm," *Air Force Magazine* 5, no. 1, January 1992. http://www.airforcemag.com/MagazineArchive/Pages/1992/January%201992/0192storm.aspx.

Mowbray, James A., "Air Force Doctrine Problems: 1926–Present," *Airpower Journal* 9, no. 4, (winter 1995): 2.

Napolitano, Janet, Department of Homeland Security, "Remarks by Secretary Napolitano before the Joint Meeting of the OSCE Permanent Council and ASCE Forum for Security Cooperation," 1 July 2011. http://www.dhs.gov/news/2011/07/01/remarks-secretary-napolitano-joint-meeting-osce-permanent-council-and-osce-forum.

"National Cyber Range Completes Beta Phase," *Air Force Magazine*, 21 November 2012. http://www.airforcemag.com/DRArchive/Pages/2012/November%202012/November%2021%202012/NationalCyberRangeCompletesBetaPhase.aspx.

National Security Archives, "National Security Strategies," May 2010. http://nssarchive.us/.

OFFICE OF AIR FORCE HISTORY WASHINGTON DC, J.S.S. *Foulois and the U.S. Army Air Corps: 1931-1935*: DIANE Publishing.

Office of the Director of National Intelligence, *The IC and Cybersecurity, Traditions, Boundaries, and Governance,* (Washington: August 2010).

O'Harrow Jr., Robert, "CyberCity allows government hackers to train for attacks," *The Washington Post*, 26 November 2012. http://articles.washingtonpost.com/2012-11-26/news/35508198_1_government-hackers-security-firm-digital-attacks.

Olsen, J.A. *John Warden and the Renaissance of American Airpower*: Potomac Books Incorporated, 2007.

Olson, M. *The Logic of Collective Action: Public Goods and the Theory of Groups*: Harvard University Press, 1965.

Op-Ed, 'Botnets' Run Wild, *Washington Post*, 24 January 2013. http://www.news-herald.com/articles/2013/01/24/opinion/nh6474510.txt.

Osinga, F.P. *Science, Strategy and War: The Strategic Theory of John Boyd*: Taylor & Francis, 2007.

Pampe, Carla, “Air Force activates cyber Numbered Air Force,” 18 August 2009.

Pape, R.A. *Bombing to Win: Airpower and Coercion in War*: Cornell University Press, 1996.

Paret, P., G.A. Craig, and F. Gilbert. *Makers of Modern Strategy from Machiavelli to the Nuclear Age*: Princeton University Press, 2008.

Peattie, M.R. *Sunburst: The Rise of Japanese Naval Airpower, 1909-1941*: Naval Inst Press, 2007.

Pellerin, Cheryl, “DOD Officials Cite Advances in Cyber Operations, Security,” *US Department of Defense: American Forces Press Service*, 14 March 2013. http://www.defense.gov/news/newsarticle.aspx?id=119532.

Perlroth, Nicole, “Washington Post Joins List of News Media Hacked by the Chinese,” *The New York Times*, 1 February 2013. http://www.nytimes.com/2013/02/02/technology/washington-posts-joins-list-of-media-hacked-by-the-chinese.html?_r=0.

Pfaltzgraff Jr., Robert, and Shultz, Jr., Richard H., “Future of Airpower in the Aftermath of the Gulf War,” Air University Press Maxwell Air Force Base, AL.

Pilkington, Ed “Washington Moves to Classify Cyber-Attacks as Acts of War,” *The Guardian*, (31 May 2011). http://www.guardian.co.uk/world/2011/may/31/washington-moves-to-classify-cyber-attacks.

Ponemon Institute, “Second Annual Cost of Cyber Crime Study,” Benchmark Study of US Companies, August 2011. http://www.hpenterprisesecurity.com/collateral/report/2011_Cost_of_Cyber_Crime_Study_August.pdf.

Putney, Diane T., “From Instant Thunder to Desert Storm: Developing the Gulf War Air Campaign’s Phases,” *Airpower History* 41, no. 3 (fall 1994).

Raleigh, W.A., and H.A. Jones. *The War in the Air: Being the Story of the Part Played in the Great War by the Royal Air Force*: Clarendon Press, 1922.

Randolph, S.P. *Powerful and Brutal Weapons: Nixon, Kissinger, and the Easter Offensive*: Harvard University Press, 2007.

Reed, John, *Foreign Policy*, “The Pentagon is tweaking the cyber capabilities it wants from the services,” 30 November 2012.

Reveron, D.S. *Cyberspace and National Security: Threats, Opportunities, and Power in a Virtual World*: Georgetown University Press, 2012.

Rid, Thomas, “Cyber War Will Not Take Place,” *The Journal of Strategic Studies* 35, no. 1 (February 2012).

Rid, Thomas, “Cyber Fail: The Obama administration’s lousy record on cyber security,” *New Republic*, 4 February 2013. http://www.newrepublic.com/article/112314/obama-administrations-louse-record-cyber-security.

Rueschhoff, Jan and Dunne, Jonathan, “Centers of Gravity from the Inside Out,” *Joint Forces Quarterly* 60, (1Q, 2011). http://www.ndu.edu/press/jfq-60.html.

Rueschhoff, Jan and Dunne, Jonathan, “US Presses China on Cyber Attacks,” *The Washington Post*, 20 March 2013. http://www.washingtonpost.com/world/asia_pacific/us-presses-china-on-cyberattacks/2013/03/20/ef11a3d0-916a-11e2-9173-7f87cda73b49_story.html.

Rumelt, R. *Good Strategy Bad Strategy: The Difference and Why It Matters*: Crown Publishing Group, 2011.

Sample, Timothy, “Calling for a National-Level Doctrine for the Cyber Era,” *Defense Systems,*18 December 2012. http://defensesystems.com/Articles/2012/12/18/special-commentary-cyber-era-doctrine.aspx?p=1.

Schelling, T.C. *Arms and Influence*: YALE University Press, 2008.

Schmitt, E., and T. Shanker. *Counterstrike: The Untold Story of America's Secret Campaign against Al Qaeda*: Henry Holt and Company, 2011.

Schmitt, M.N. *Tallinn Manual on the International Law Applicable to Cyber Warfare*: Cambridge University Press, 2013.

Segal, Adam, Greenberg, Maurice, and Waxman, Matthew, “Why a Cybersecurity Treaty Is a Pipe Dream,” *Council on Foreign Relations*, 27 October, 2011. http://www.cfr.org/cybersecurity/why-cybersecurity-treaty-pipe-dream/p26325.

Serbu, Jared, “Air Force role just 1 piece of DOD’s cyber puzzle,” *Federal News Radio,* 3 Dec 12, 2. http://www.federalnewsradio.com/398/3140801/Air-Force-gels-around-its-cyber-future.

Sheldon, John B., “State of the Art: Attackers and Targets in Cyberspace,” *Journal of Military and Strategic Studies* 14, no.2, 2012.

Sherry, P.M.S. *The Rise of American Airpower: The Creation of Armageddon*: Yale University Press, 1987.

Shwedo, Brigadier General Brad, Interview with author, 2 November 2012.

Strange, Doctor Joe and Iron, Colonel Richard (UKA), “Understanding Centers of Gravity and Critical Vulnerabilities: Part 1. http://www.au.af.mil/au/awc/awcgate/usmc/cog1.pdf.

Strassler, R.B., and V.D. Hanson. *The Landmark Thucydides: A Comprehensive Guide to the Peloponnesian War*: Simon & Schuster, 1998.

Suffolk, John, “Cyber Security Perspectives,” *Huawei*, September 2012, 10, http://www.huawei.com/ilink/en/download/HW_187368.

Sunzi, S.T.S.B.G. *The Illustrated Art of War: The Definitive English Translation by Samuel B. Griffith*: Oxford University Press, 2005.

Tanaka, Y., and M.B. Young. *Bombing Civilians: A Twentieth-Century History*: NEW Press, 2010.

Tooze, J.A. *The Wages of Destruction: The Making and Breaking of the Nazi Economy*: Penguin Books, 2008.

Twenty-Fourth Air Force, (Draft) “Twenty-Fourth Air Force Weapons and Tactics Roadmap,” 2011.

Tyson, N.G., and A. Lang. *Space Chronicles: Facing the Ultimate Frontier*: W. W. Norton, 2012.

United Nations Charter, United Nations and Security Council, Chapter VII, Article 39. http://www.un.org/en/documents/charter/chapter7.shtml.

United Press International, “Israel Builds up its Cyberwar Corps,” 2 November 2012. http://www.upi.com/Business_News/Security-Industry/2012/11/02/Israel-builds-up-its-cyberwar-corps/UPI-52421351881449.

United States Marine Corps, Marine Corps Document Publicatoin – 1, *Warfighting*, 20 June 1997.

United States of America, *National Space Policy,* (Washington, DC: Office of the President of the United States, 28 June 2010).

United States of America, 2013 National Defense Authorization Act, "One Hundred Twelfth Congress of the United States," 3 January 2012. http://www.gpo.gov/fdsys/pkg/BILLS-112hr4310enr/pdf/BILLS-112hr4310enr.pdf.

United States Code, *Title 50—War and National Defense,* USC 50 § 932, 4 January 2012. http://www.law.cornell.edu/uscode/pdf/lii_usc_TI_50.pdf.

Valeri, Lorenzo, "Countering Threats in Space and Cyberspace: A Proposed Combined Approach," (Chatham House: January 2013). http://www.chathamhouse.org/sites/default/files/public/Research/International%20Security/0113discussionpaper_Valeri.pdf.

Vautrinot, Major General Suzanne, "Sharing the Cyber Journey," *Strategic Studies Quarterly* 6, no.3 (Fall 2012).

Waltz, K.N. *Man, the State, and War: A Theoretical Analysis*: Columbia University Press, 2001.

———. *Theory of International Politics*: Waveland PressInc, 2010.

Walzer, P.M. *Just and Unjust Wars: A Moral Argument with Historical Illustrations*: BasicBooks, 2006.

Warden III, Colonel (r) John A. *The Air Campaign: Planning for Combat*: iUniverse, 2000.

Warden III., Colonel (r) John A., Interview by author, 30 January, 2013; Montgomery AL.

Watts, Barry D., "The Foundations of US Air Doctrine: The Problem of Friction in War," (Maxwell AFB, Ala.: Air University Press, 1984).

Waxman, Matthew, "Cyber-Attacks and the Use of Force: Back to the Future of Article 2(4)," *Yale Journal of International Law* 36, no.2 (Fall 2010). http://www.yjil.org/docs/pub/36-2-waxman-cyber-attacks-and-the-use-of-force.pdf.

Webster's Student Dictionary (Trident International Press, 1999).

Weisgerber, Marcus, "Report: DOD Could Save Billions with New Military Strategy," *DefenseNews*, 15 November 2012. http://www.defensenews.com/article/20121115/DEFREG02/311150001/Report-DoD-Could-Save-Billions-New-Military-Strategy.

Wells, H.G. *The War in the Air*: Boni and Liveright, Incorporated, 1917.

Welch, General (r) Larry, IDA Research Notes, "Challenges in Cyberspace," Summer 2011. https://www.ida.org/upload/research%20notes/researchnotessummer2011.pdf.

Welch, Paul, Commander, 688th Information Operations Wing, Telephone interview with author, 12 December 2012.

Welsh III., General Mark A., "A Vision for the United States Air Force," 2013 Air Force Mission Statement. http://www.posturestatement.af.mil/main/welcome.asp.

Welsh III.,General Mark A., Air Force Association Air & Space Conference and Technology Exposition on 18 September 2012. http://www.af.mil/shared/media/document/AFD-120928-037.pdf.

White Jr., Lynn, *Medieval Technology & Social Change*, (Oxford University Press: 1964).

Williams, Brett, “Ten Propositions Regarding Cyberspace Operations,” *Joint Forces Quarterly* 61, (2Q, 2011).

Winton, Harold, “An Imperfect Jewel: Military Theory and the Military Profession,” *The Journal of Strategic Studies* 34, no.6.

Xiaoming Zhang, J.G.D. *Red Wings over the Yalu: China, the Soviet Union, and the Air War in Korea*: Texas A&M University Press, 2003.